Modicon MCSESM, MCSESP Series

Managed Switch

Configuration Guide

Original instructions

QGH59056.03
02/2026

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

⚡ The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

⚠ This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER
DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING
WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION
CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE
NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

Before You Begin

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions, government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point-of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

Start-up and Test

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check are made and that enough time is allowed to perform complete and satisfactory testing.

⚠WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995:

(In case of divergence or contradiction between any translation and the English original, the original text in the English language will prevail.)

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer’s instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer’s instructions and the machinery used with the electrical equipment.
- Only those operational adjustments required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

About the Document

Document Scope

This document describes how to configure the Modicon MCSESM, MCSESP series managed switches.

Validity Note

This document has been updated for the release of the firmware versions available at the publication date of this document.

Product Related Information

⚠WARNING

LOSS OF CONTROL

- Perform a Failure Mode and Effects Analysis (FMEA), or equivalent risk analysis, of your application, and apply preventive and detective controls before implementation.
- Provide a fallback state for undesired control events or sequences.
- Provide separate or redundant control paths wherever required.
- Supply appropriate parameters, particularly for limits.
- Review the implications of transmission delays and take actions to mitigate them.
- Review the implications of communication link interruptions and take actions to mitigate them.
- Provide independent paths for control functions (for example, emergency stop, over-limit conditions, and error conditions) according to your risk assessment, and applicable codes and regulations.
- Apply local accident prevention and safety regulations and guidelines.[1]
- Test each implementation of a system for proper operation before placing it into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[1] For additional information, refer to NEMA ICS 1.1 (latest edition), "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control" and to NEMA ICS 7.1 (latest edition), "Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems" or their equivalent governing your particular location.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Only use software and hardware components approved by Schneider Electric for use with the system.
- Update your application program every time you change the physical hardware configuration.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the Cybersecurity Best Practices document.

Schneider Electric provides additional information and assistance:

- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity posture.
  - Learn more about cybersecurity in the cybersecurity academy.
  - Explore the cybersecurity services from Schneider Electric.

Environmental Data

For product compliance and environmental information, refer to the Schneider Electric Environmental Data Program.

Available Languages of the Document

The document is available in these languages:

- English (QGH59056)
- French (QGH59080)
- German QGH59058
- Spanish (QGH59081)
- Italian (QGH59082)
- Chinese (QGH59083)

Related Documents

Title of documentation	Reference number
Modicon MCSESM, MCSESP Series Managed Switch Installation Guide	QGH59091 (EN) QGH59094 (FR) QGH59093 (DE) QGH59096 (IT) QGH59095 (ES) QGH59097 (CN)
Modicon MCSESM, MCSESP Series Managed Switch Graphic User Interface User Guide	QGH59084 (EN) QGH59087 (FR) QGH59086 (DE) QGH59089 (IT) QGH59088 (ES) QGH59090 (CN)

Title of documentation	Reference number
Modicon MCSESM, MCSESP Series Managed Switch Command Line Interface User Guide	QGH59098 (EN)
Modicon MCSESM, MCSESP Series Managed Switch Security User Guide	EIO0000005492 (EN) EIO0000005493 (FR) EIO0000005494 (DE) EIO0000005495 (IT) EIO0000005496 (ES) EIO0000005497 (CN)

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Terminology Derived from Standards

The technical terms, terminology, symbols and the corresponding descriptions in the information contained herein, or that appear in or on the products themselves, are generally derived from the terms or definitions of international standards.

In the area of functional safety systems, drives and general automation, this may include, but is not limited to, terms such as *safety*, *safety function*, *safe state*, *fault*, *fault reset*, *malfunction*, *failure*, *error*, *error message*, *dangerous*, etc.

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers, part 2: Equipment requirements and tests.
ISO 13849-1:2023	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2020	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design
IEC 62061:2021	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software requirements.
IEC 61784-3:2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.

Standard	Description
2006/42/EC	Machinery Directive
2014/30/EU	Electromagnetic Compatibility Directive
2014/35/EU	Low Voltage Directive

In addition, terms used in the present document may tangentially be used as they are derived from other standards such as:

Standard	Description
IEC 60034 series	Rotating electrical machines
IEC 61800 series	Adjustable speed electrical power drive systems
IEC 61158 series	Digital data communications for measurement and control – Fieldbus for use in industrial control systems

Finally, the term *zone of operation* may be used in conjunction with the description of specific hazards, and is defined as it is for a *hazard zone* or *danger zone* in the *Machinery Directive* (*2006/42/EC*) and *ISO 12100:2010*.

NOTE: The aforementioned standards may or may not apply to the specific products cited in the present documentation. For more information concerning the individual standards applicable to the products described herein, see the characteristics tables for those product references.

User Interfaces

The device has the following user interfaces:

User interface	Requires authorization	Accessible through …	Prerequisite
Graphical User Interface, page 18	Yes	Ethernet	Web browser
Command Line Interface, page 19	Yes	Ethernet	SSH client
		Serial interface	VT100 terminal emulator
System Monitor 1, page 33	No	Serial interface	

Authorization to access the device management is assigned in the following ways:

- With a user account set up on the device

  Refer to User Management, page 49
- A remote server grants authorization
  - RADIUS
  - LDAP, see LDAP Function, page 57
  - TACACS+, see TACACS+, page 66

Graphical User Interface

System Requirements

To access the device management using the Graphical User Interface, you need a web browser with HTML5 support.

Web browsers and other third-party software routinely validate digital certificates. If your web browser displays a message indicating a conflict in validating the digital certificate of the device, perform the following steps:

- Verify if the digital certificate of the device has expired.
- Verify if your web browser still considers that the digital certificate is trustworthy.

To solve the conflict in validation, regenerate the digital certificate on the device using the latest device software. As an alternative, generate a digital certificate externally, using up-to-date signature algorithms. Transfer the new digital certificate onto the device.

Access to Device Management

The prerequisite for accessing device management is that the IP parameters are set up in the device. Specifying the IP Parameters, page 37

Perform the following steps:

- Start the web browser on the PC.
- Type the IP address of the device in the address field of the web browser.

  The web browser sets up the connection to the device and displays the login dialog.
- When you want to change the language of the Graphical User Interface, click the appropriate link in the top right corner of the login dialog.

- Enter the user name and password.
  - The default user name is **admin**.
  - The default password is **private**.

    When you enter the default password during the initial setup of the device, the device will prompt you to enter a new password.

    First Login (Password Change), page 47
- Click **Login**.

  If the credentials are correct, you are logged in to the device management.

Command Line Interface

The Command Line Interface provides an environment for configuring IT devices.

You can access the device management using the Command Line Interface in the following ways:

- Through the serial connection, page 19
- Over the network using Secure Shell (SSH), page 20

You find information about assembling and starting up the device in the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*. For Command Line Interface, also refer to the *Modicon MCSESM, MCSESP Series Managed Switch Command Line Interface User Guide*.

Access to Device Management Through the Serial Connection

To access the device management, connect a PC with VT100 terminal emulator to the serial interface of the device.

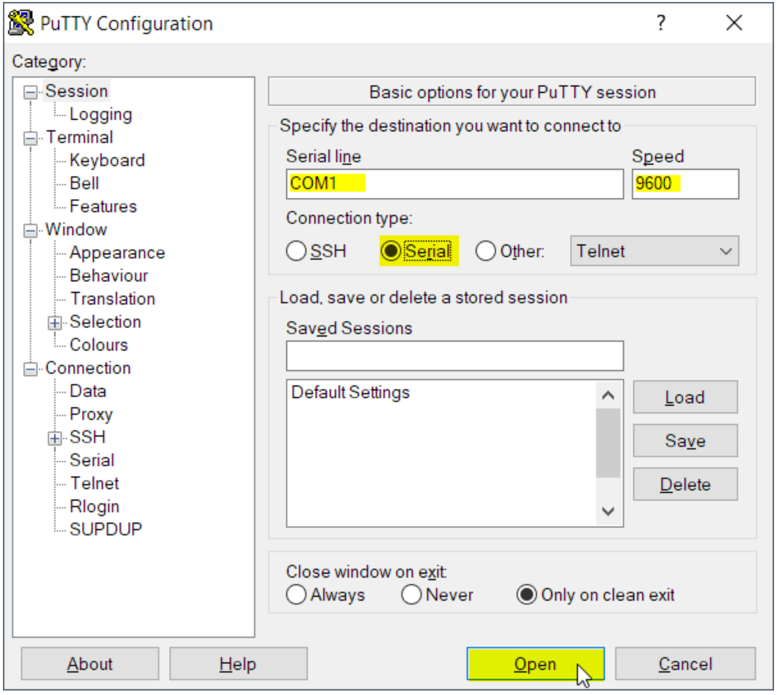
VT100 terminal emulator settings	
Speed	**9600 bit/s**
Data	**8 bit**
Stopbit	**1 bit**
Parity	**None**
Handshake	**None**

The following example guides you through the necessary steps using the PuTTY application as VT100 terminal emulator. PuTTY is a free implementation of SSH and Telnet for Windows and Unix platforms, along with an xterm terminal emulator.

Perform the following steps:

- Connect the PC to the serial interface of the device.
- On the PC, start the VT100 terminal emulator.

- Set up the serial connection, then click **Open**.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM1

Speed: 9600

Connection type: ○ SSH ● Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

- Press any key on the keyboard repeatedly.

  After a few seconds, the VT100 terminal emulator displays the login screen.
- Enter the user name and password.
  - The default user name is **admin**.
  - The default password is **private**.

    When you enter the default password during the initial setup of the device, the device will prompt you to enter a new password. Also refer to First Login (Password Change), page 47.

You are logged in to the device management.

The start screen of the command line interface provides the following information:

```
Copyright (c) 2011-2025 Schneider Electric SE
All rights reserved
MCSESM Release 99.9.00
(Build date 2025-09-20 06:33)
 System Name:MCSESM-646038d6e958
 Management IP:192.168.1.5
 Subnet Mask:255.255.255.0
 Base MAC:64:60:38:01:02:03
 USB IP:91.0.0.100
 USB Mask:255.255.255.0
 System Time:2025-09-22 09:44:29
NOTE: Enter '?' for Command Help. Command help displays all options
that are valid for the particular mode.
For the syntax of a particular command form, please
consult the documentation.
MCSESM>
```

Access to the Device Management Using SSH

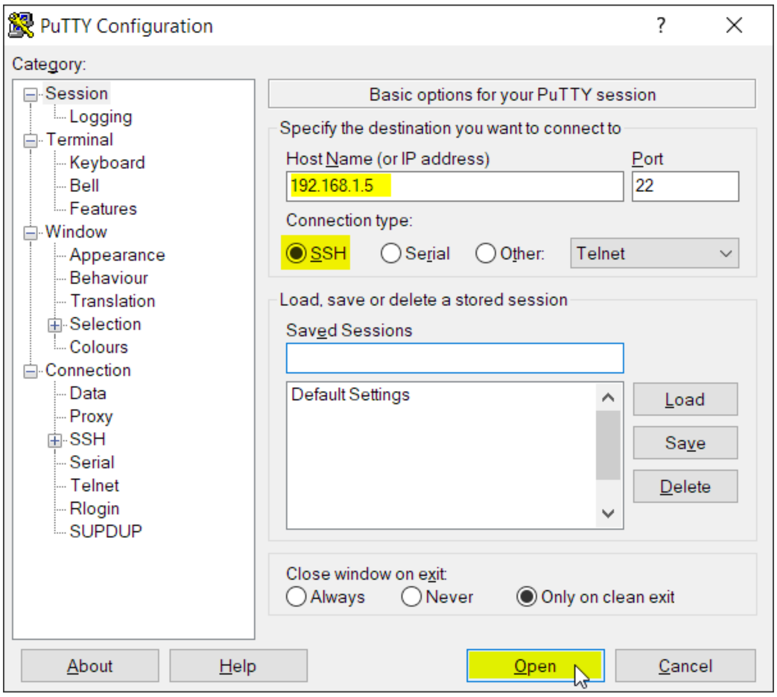
The prerequisite for accessing device management is that the IP parameters are set up in the device. Refer to Specifying the IP Parameters, page 37.

The following example guides you through the necessary steps using the PuTTY application as the SSH client. PuTTY is a free implementation of SSH and Telnet for Windows and Unix platforms, along with an xterm terminal emulator. As an alternative, you can use the `ssh` command, which is part of OpenSSH.

Perform the following steps:

- Connect the PC to the device over the Ethernet network.

- On the PC, start the SSH client application.
- Set up the SSH connection.



PuTTY Configuration

Host Name (or IP address): 192.168.1.5

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Close window on exit: ○ Always ○ Never ● Only on clean exit

- In the **Host Name (or IP address)** field, enter the IP address of the device.
- In the **Connection type** option list, select the **SSH** radio button.
- Click **Open**.

  When you connect the PC to the device for the first time, the SSH client application displays a *host key* verification message.

  - Verify the fingerprint of the key the SSH server of the device sends.

    NOTE: On the device, you can display the fingerprint of the *host key* with the command `show ssh server` or in the **Device Security > Management Access > Server**, **SSH** tab.

  - To continue, accept the key.

  Establishing the connection takes a few seconds.

- Enter the user name and password.
  - The default user name is **admin**.
  - The default password is **private**.

    When you enter the default password during the initial setup of the device, the device prompts you to enter a new password. See First Login (Password Change), page 47.

You are logged in to the device management.

The start screen of the command line interface provides the following information:

```
login as: admin
admin@192.168.1.5's password:
Copyright (c) 2011-2025 Schneider Electric SE
All rights reserved
MCSESM Release 99.9.00
(Build date 2025-09-20 06:33)
 System Name:MCSESM-646038d6e958
 Management IP:192.168.1.5
 Subnet Mask:255.255.255.0
 Base MAC:64:60:38:01:02:03
 USB IP:91.0.0.100
 USB Mask:255.255.255.0
 System Time:2025-09-22 09:44:29
NOTE: Enter '?' for Command Help. Command help displays all options
that are valid for the particular mode.
For the syntax of a particular command form, please
consult the documentation.
MCSESM>
```

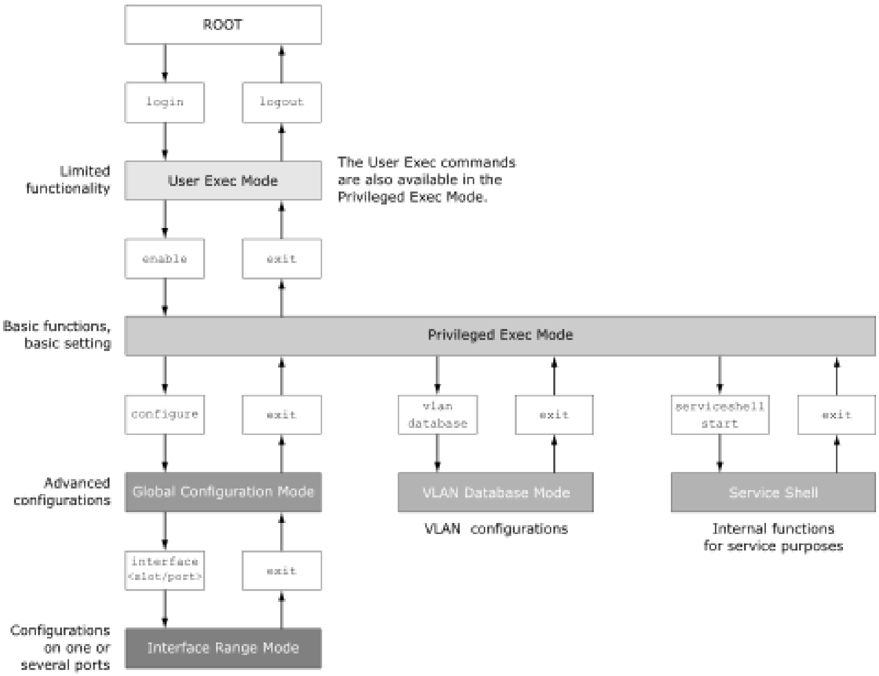
Mode-Based Command Hierarchy

In the Command Line Interface, the commands are grouped into operational modes.

Each mode provides access to the command types relevant to that mode. The commands available to you depend on both your user role (administrator, operator, auditor, guest) and the mode you are working in.

When you change to a specific mode, only the commands associated with that mode become available. *User Exec* mode is the only exception: its commands can also be executed in *Privileged Exec* mode.

The following figure illustrates the structure of the CLI modes.



The Command Line Interface supports the following modes:

Command Mode	Prompt	Description
User Exec	`(MCSESM) >`	When you log into the device management with the Command Line Interface, you are in the *User Exec* mode. The *User Exec* mode contains a limited range of commands.
Privileged Exec	`(MCSESM) #`	To access the entire range of commands, you change to the *Privileged Exec* mode. The prerequisite for changing to the *Privileged Exec* mode is that you log into the device management as a privileged user. In the *Privileged Exec* mode, you are also able to execute the *User Exec* mode commands.
VLAN mode	`(MCSESM) (VLAN)#`	The VLAN mode contains VLAN-related commands.
Service Shell	`/mnt/fastpath #`	The Service Shell is for service purposes only.
Global Config	`(MCSESM) (config)#`	The Global Config mode allows modifications to the present configuration. This mode groups general setup commands.

Command Mode	Prompt	Description
Interface Range	–	The commands in the Interface Range mode affect a specific port, a selected group of multiple ports or all ports of the device. The commands modify a value or switch a function on/off on one or more specific ports.

	`(MCSESM) ((interface) all)#`	All physical ports in the device
		Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
		`(MCSESM) (config)#interface all`
		`(MCSESM) ((Interface)all)#`

	`(MCSESM) (interface <slot/port>)#`	A single port on one interface
		Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
		`(MCSESM) (config)#interface 2/1`
		`(MCSESM) (interface 2/1)#`

	`(MCSESM) (interface <interface range> )#`	A range of ports on one interface
		Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
		`(MCSESM) (config)#interface 1/2-1/4`
		`(MCSESM) ((Interface)1/2-1/4)#`

	`(MCSESM) (interface <interface list>)#`	A list of single ports
		Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
		`(MCSESM) (config)#interface 1/2,1/4,1/5`
		`(MCSESM) ((Interface)1/2,1/4,1/5)#`

	`(MCSESM) (interface <complex range>)#`	A list of port ranges and single ports
		Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
		`(MCSESM) (config)#interface 1/2-1/4,1/6-1/9`
		`(MCSESM) ((Interface)1/2-1/4,1/6-1/9)#`

The following table displays the command modes, the command prompts (input request characters) visible in the corresponding mode, and the option with which you quit this mode.

Command Mode	Access Method	Quit or start next mode

User Exec	First access level. Perform basic tasks and list system information.	To quit, you enter `logout`:
		`(MCSESM) >logout`
		`Are you sure (Y/N) ?y`

Privileged Exec	From the *User Exec* mode, you enter the command `enable`:
	`(MCSESM) >enable`
	`(MCSESM) #`
		To quit the *Privileged Exec* mode and return to the *User Exec* mode, you enter `exit`:
		`(MCSESM) #exit`
		`(MCSESM) >`

VLAN	From the *Privileged Exec* mode, you enter the command `vlan database`:
	`(MCSESM) #vlan database`
	`(MCSESM) (Vlan)#`
		To quit the *VLAN* mode and return to the *Privileged Exec* mode, you enter `exit` or press **Ctrl+Z**:
		`(MCSESM) (Vlan)#exit`
		`(MCSESM) #`

Command Mode	Access Method	Quit or start next mode

Global Config	From the *Privileged Exec* mode, you enter the command `configure`:
	`(MCSESM) #configure`
	`(MCSESM) (config)#`
	From the *User Exec* mode, you enter the command `enable` and then in the *Privileged Exec* mode, you enter the command `configure`:
	`(MCSESM) >enable`
	`(MCSESM) #configure`
	`(MCSESM) (config)#`
		To quit the *Global Config* mode and return to the *Privileged Exec* mode, you enter `exit`:
		`(MCSESM) (config)#exit`
		`(MCSESM) #`
		To then quit the *Privileged Exec* mode and return to the *User Exec* mode, you enter `exit` again:
		`(MCSESM) #exit`
		`(MCSESM) >`

Interface Range	From the *Global Config* mode, you enter the command `interface {all|<slot/port>|<interface range> |<interface list>|<complex range>}`.
	`(MCSESM) (config) #interface<slot/port>`
	`(MCSESM) (interface slot/port) #`
		To quit the *Interface Range* mode and return to the *Global Config* mode, you enter `exit`. To return to the *Privileged Exec* mode, you press **Ctrl+Z**.
		`(MCSESM) (interface slot/port) #exit`
		`(MCSESM) #`

When you enter a question mark (?) after the prompt, the Command Line Interface displays a list of the available commands and a short description of the commands.

Example of commands in the *User Exec* mode:

```
(MCSESM)>
  cli      Set the CLI preferences.
  enable   Turn on privileged commands.
  help     Display help for various special keys.
  history  Show a list of previously run commands.
  logout   Exit this session.
  ping     Send ICMP echo packets to a specified IP address.
  show     Display device options and settings.
  telnet   Establish a telnet connection to a remote host.
(MCSESM)>
```

Executing a Command

Syntax Analysis

When you log into the device management with the Command Line Interface, you are in the *User Exec* mode. The Command Line Interface displays the prompt `(MCSESM)>` on the screen.

When you enter a command and press the **Enter** key, the Command Line Interface starts the syntax analysis. The Command Line Interface searches the command tree for the desired command.

When the command is outside the Command Line Interface command range, a message informs you of the detected error.

Example:

You want to execute the `show system info` command, but enter `info` without `f` and press the **Enter** key.

The Command Line Interface then displays the message:

```
(MCSESM)>show system ino
```

```
Error: Invalid command 'ino'
```

Command Tree

The commands in the Command Line Interface are organized in a tree structure. The commands, and where applicable the related parameters, branch down until the command is completely defined and therefore executable. The Command Line Interface verifies the input. When you entered the command and the parameters correctly and completely, you execute the command with the **Enter** key.

After you entered the command and the required parameters, the other parameters entered are treated as optional parameters. When one of the parameters is undefined, the Command Line Interface displays a syntax message.

The command tree branches for the required parameters until the required parameters have reached the last branch in the structure.

With optional parameters, the command tree branches until the required parameters and the optional parameters have reached the last branch in the structure.

Structure of a Command

This section describes the syntax, conventions and terminology, and uses examples to represent them.

Format of Commands

Most of the commands include parameters.

When the command parameter is missing, the Command Line Interface informs you about the detection of an incorrect command syntax.

This manual displays the commands and parameters in the **Courier** font.

Parameters

The sequence of the parameters is relevant for the correct syntax of a command.

Parameters are required values, optional values, selections, or a combination of these things. The following table presents the command syntax of parameters:

Parameter	Command syntax
`<command>`	Commands in pointed brackets (**<>**) are mandatory.
`[command]`	Commands in square brackets (**[]**) are optional.
`<parameter>`	Parameters in pointed brackets (**<>**) are mandatory.
`[parameter]`	Parameters in square brackets (**[]**) are optional.
`...`	An ellipsis after an element indicates that you can repeat the element.
`[Choice1 | Choice2]`	A vertical line enclosed in brackets indicates a selection option. Select one value. Elements separated by a vertical line and enclosed in square brackets indicate an optional selection (Choice1, Choice2, or no selection).
`{list}`	Curved brackets (**{}**) indicate that a parameter is to be selected from a list of options.
`{Choice1 | Choice2}`	Elements separated by a vertical line and enclosed in curved brackets (**{}**) indicate a mandatory selection (either Choice1 or Choice2).
`[param1 {Choice1 | Choice2}]`	Displays an optional parameter that contains a mandatory selection.

Parameter	Command syntax
`<a.b.c.d>`	Lowercase letters are wild cards. You enter parameters with the notation a.b.c.d with decimal points (for example IP addresses)
`<cr>`	You press the **Enter** key to insert a line break (carriage return).

The following table presents the possible parameter values within the Command Line Interface:

Value	Description
IP address	This parameter represents a valid IPv4 address. The address consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by a decimal point. The IP address **0.0.0.0** is a valid entry.
MAC address	This parameter represents a valid MAC address. The address consists of 6 hexadecimal numbers with values from 00 to FF. The numbers are separated by a colon, for example, **00:F6:29:B2:81:40**.
string	User-defined text with a length in the specified range, for example a maximum of 32 characters.
character string	Use double quotation marks to indicate a character string, for example **“System name with space character”**.
number	Whole integer in the specified range, for example **0..999999**.
date	Date in format **YYYY-MM-DD**.
time	Time in format **HH:MM:SS**.

Network Addresses

Network addresses are a requirement for establishing a data connection to a remote work station, a server, or another network. You distinguish between IP addresses and MAC addresses.

The IP address is an address allocated by the network administrator. The IP address is unique in one network area.

The MAC addresses are assigned by the hardware manufacturer.

The following table presents the format and the range of the address types:

Address Type	Format	Range	Example
IP address	nnn.nnn.nnn.nnn	nnn: 0 to 255 (decimal)	192.168.11.110
MAC address	mm:mm:mm:mm:mm:mm	mm: 00 to ff (hexadecimal number pairs)	A7:C9:89:DD:A9:B3

Strings

A string is indicated by quotation marks. For example, **“System name with space character”**. Space characters are not valid user-defined strings. You enter a space character in a parameter between quotation marks.

Example:

```
*(MCSESM)#cli prompt Device name
Error: Invalid command 'name'
*(MCSESM)#cli prompt 'Device name'
*(Device name)#
```

Examples of Commands

Example 1: clear arp-table-switch

Command for clearing the ARP table of the management agent (cache).

`clear arp-table-switch` is the command name. The command is executable without any other parameters by pressing the **Enter** key.

Example 2: radius server timeout

Command to specify the RADIUS server timeout value.

```
(MCSESM) (config)#radius server timeout
 <1..30>                Timeout in seconds (default: 5).
```

`radius server timeout` is the command name.

The parameter is required. The value range is **1..30**.

Example 3: radius server auth modify <1..8>

Command to set the parameters for RADIUS authentication server 1.

```
(MCSESM) (config)#radius server auth modify 1
 [name]                 RADIUS authentication server name.
 [port]                 RADIUS authentication server port.
                        (default: 1812).
 [msgauth]              Enable or disable the message
authenticator
                        attribute for this server.
 [primary]              Configure the primary RADIUS server.
 [status]               Enable or disable a RADIUS
authentication
                        server entry.
 [secret]               Configure the shared secret for the
RADIUS
                        authentication server.
 [encrypted]            Configure the encrypted shared
secret.
  <cr>                  Press Enter to execute the command.
```

`radius server auth modify` is the command name.

The parameter **<1..8>** (RADIUS server index) is required. The value range is **1..8** (integer).

The parameters **[name]**, **[port]**, **[msgauth]**, **[primary]**, **[status]**, **[secret]** and **[encrypted]** are optional.

Input Prompt

Command Mode

With the input prompt, the Command Line Interface displays which of the three modes you are in:

- `(MCSESM) >`

  User Exec mode
- `(MCSESM) #`

  Privileged Exec mode
- `(MCSESM) (config)#`

  Global Config mode

- `(MCSESM) (Vlan)#`

  VLAN Database mode
- `(MCSESM) ((Interface)all)#`

  Interface Range mode / All ports of the device
- `(MCSESM) ((Interface)2/1)#`

  Interface Range mode / A single port on one interface
- `(MCSESM) ((Interface)1/2-1/4)#`

  Interface Range mode / A range of ports on one interface
- `(MCSESM) ((Interface)1/2,1/4,1/5)#`

  Interface Range mode / A list of single ports
- `(MCSESM) ((Interface)1/1-1/2,1/4-1/6)#`

  Interface Range mode / A list of port ranges and single ports

Asterisk, Pound Sign and Exclamation Mark

- Asterisk `*`

  An asterisk `*` in the first or second position of the input prompt means that the settings in the volatile memory and the settings in the non-volatile memory are different. In your configuration, the device has detected modifications which have not been saved.

  `*(MCSESM)>`
- Pound sign `#`

  A pound sign `#` at the beginning of the input prompt means that the boot parameters and the parameters during the boot phase are different.

  *#`(MCSESM)>`
- Exclamation mark `!`

  An exclamation mark `!` at the beginning of the input prompt means that the password for the **admin** user account corresponds with the default setting.

  `!(MCSESM)>`

Wildcards

The device allows the command line prompt to be changed.

The Command Line Interface supports the following wildcards within the input prompt:

Wildcard	Description
%d	System date
%t	System time
%i	IP address of the device
%m	MAC address of the device
%p	Product name of the device

Input prompts examples:

```
!(MCSESM)>enable
!(MCSESM)#cli prompt %i
!192.168.1.5#cli prompt (MCSESM)%d
!*(MCSESM)2025-09-22#cli prompt (MCSESM)%d%t
!*(MCSESM)2025-09-22 09:44:29#cli prompt %m
!*AA:BB:CC:DD:EE:FF#
```

Key Combinations

The following key combinations help you work with the Command Line Interface:

Key combination	**Description**
CTRL + **H**, **Backspace**	Delete previous character
CTRL + **A**	Go to beginning of line
CTRL + **E**	Go to end of line
CTRL + **F**	Go forward one character
CTRL + **B**	Go backward one character
CTRL + **D**	Delete present character
CTRL + **U**, **X**	Delete to beginning of line
CTRL + **K**	Delete to end of line
CTRL + **W**	Delete previous word
CTRL + **P**	Go to previous line in history buffer
CTRL + **R**	Rewrite or paste the line
CTRL + **N**	Go to next line in history buffer
CTRL + **Z**	Return to root command prompt
CTRL + **G**	Aborts running tcpdump session
Tab + **Spacebar**	Command line completion
`Exit`	Go to next lower command prompt
?	List choices

The Help command displays the possible key combinations in Command Line Interface on the screen:

```
(MCSESM) #help
HELP:
Special keys:
  Ctrl-H, BkSp delete previous character
  Ctrl-A  .... go to beginning of line
  Ctrl-E  .... go to end of line
  Ctrl-F  .... go forward one character
  Ctrl-B  .... go backward one character
  Ctrl-D  .... delete current character
  Ctrl-U, X .. delete to beginning of line
  Ctrl-K  .... delete to end of line
  Ctrl-W  .... delete previous word
  Ctrl-P  .... go to previous line in history buffer
  Ctrl-R  .... rewrites or pastes the line
  Ctrl-N  .... go to next line in history buffer
  Ctrl-Z  .... return to root command prompt
  Ctrl-G  .... aborts running tcpdump session
  Tab, <SPACE> command-line completion
  Exit    .... go to next lower command prompt
  ?       .... list choices
(MCSESM) #
```

Data Entry Elements

Command Completion

To simplify typing commands, the Command Line Interface allows command completion (Tab Completion). Thus you are able to abbreviate keywords.

- Type in the beginning of a keyword. When the characters entered identify a keyword, the Command Line Interface completes the keyword after you press the **Tab** key or the **Spacebar** key. When there is more than one option for completion, enter the letter or the letters necessary for uniquely identifying the keyword. Press the **Tab** key or the **Spacebar** again. After that, the system completes the command or parameter.
- When you make a non-unique entry and press the **Tab** key or the **Spacebar** twice, the Command Line Interface provides you with a list of options.
- On a non-unique entry and pressing the **Tab** key or the **Spacebar**, the Command Line Interface completes the command up to the end of the uniqueness. When several commands exist and you press the **Tab** key or the **Spacebar** again, the Command Line Interface provides you with a list of options.

  Example:

  ```
  (MCSESM) (Config)#lo
  ```

  ```
  (MCSESM) (Config)#log
  ```

  ```
  logging logout
  ```

  When you enter **lo** + **Tab** + **Spacebar**, the Command Line Interface completes the command up to the end of the uniqueness to `log`.

  When you press the **Tab** key or the **Spacebar** again, the Command Line Interface provides you with a list of options (`logging logout`).

Possible Commands/Parameters

You can obtain a list of the commands or the possible parameters by entering `help` or `?`, for example by entering `(MCSESM) >show ?`

When you enter the command displayed, you get a list of the parameters available for the command `show`.

When you enter the command without space character in front of the question mark, the device displays the help text for the command itself:

```
!*#(MCSESM)(Config)#show?
```

```
show Display device options and settings.
```

Use Cases

Saving the Configuration

To help ensure that your password settings and your other configuration changes are kept after the device is reset or after an interruption of the voltage supply, you save the configuration. To do this, perform the following steps:

- Enter `enable` to change to the *Privileged Exec* mode.
- Enter the following command:

  ```
  save [profile]
  ```

- Execute the command by pressing the **Enter** key.

Syntax of the `radius server auth add` Command

Use this command to add a RADIUS authentication server.

- Mode: Global Config mode
- Privilege Level: **administrator**

- Format: `radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
  - **[name]**: RADIUS authentication server name.
  - **[port]**: RADIUS authentication server port (default value: **1813**).

Parameter	Description	Possible values
`<1..8>`	RADIUS server index.	**1..8**
`<a.b.c.d>`	RADIUS accounting server IP address.	IP address
`<string>`	Enter a user-defined text, max. 32 characters.	
`<1..65535>`	Enter port number between 1 and 65535.	**1..65535**

Mode and Privilege Level:

- Prerequisites for executing the command:
  - You are in the Global Config mode.

    Mode-Based Command Hierarchy, page 22
  - You have the access role **administrator**.

Syntax of commands and parameters: Structure of a Command, page 25

Examples for executable commands:

- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`

Service Shell

The Service Shell is for service purposes only.

The Service Shell gives users access to internal functions of the device. When you need assistance with your device, the service personnel use the Service Shell to monitor internal conditions for example, the switch or controller registers.

NOTICE

INOPERABLE EQUIPMENT

Do not execute internal functions without service technician instructions.

Failure to follow these instructions can result in equipment damage.

Start the Service Shell

The prerequisite is that you are in *User Exec* mode: `(MCSESM) >`

Perform the following steps:

- Enter `enable` and press **Enter**.

  To reduce the effort when typing:
  - Enter `e` and press the **Tab** key.

- Enter `serviceshell start` and press **Enter**.

  To reduce the effort when typing:

  - Enter `ser` and press the **Tab** key.
  - Enter `s` and press the **Tab** key.

Examples:

```
!MCSESM >enable
!*MCSESM #serviceshell start
 WARNING! The service shell offers advanced diagnostics and functions.
 Proceed only when instructed by a service technician.
 You can return to the previous mode using the 'exit' command.
 BusyBox v1.31.0 (2025-09-22 09:44:29 UTC) built-in shell (ash)
 Enter 'help' for a list of built-in commands.
!/mnt/fastpath #
```

Working with the Service Shell

When the Service Shell is active, the timeout of the Command Line Interface is inactive. To help prevent configuration inconsistencies, end the Service Shell before any other user starts transferring a new configuration to the device.

Display the Service Shell Commands

The prerequisite is that you already started the Service Shell.

Perform the following step:

- Type `help` and press the **Enter** key.

Result: The displayed commands are:

```
/mnt/fastpath # help
Built-in commands:
------------------
        . : [ [[ alias bg break cd chdir command continue echo eval exec
        exit export false fg getopts hash help history jobs kill let
        local pwd read readonly return set shift source test times trap
        true type ulimit umask unalias unset wait
/mnt/fastpath #
```

End the Service Shell

Perform the following step:

- Enter `exit` and press the **Enter** key.

Deactivate the Service Shell Permanently in the Switch

When you deactivate the Service Shell, you are still able to configure the device. However, you limit the possibilities of service personnel to perform system diagnostics. The service technician will no longer be able to access internal functions of your device.

The deactivation is irreversible. The Service Shell remains permanently deactivated. **To reactivate the Service Shell, the device requires disassembly by the manufacturer.**

The prerequisites are:

- The Service Shell is not started.
- You are in *User Exec* mode: `(MCSESM) >`

Perform the following steps:

- Enter `enable` and press **Enter** .

  To reduce the effort when typing:

  - Enter **e** and press the **Tab** key.
- Enter `serviceshell deactivate` and press **Enter**.

  To reduce the effort when typing:

  - Enter **ser** and press the **Tab** key.
  - Enter **dea** and press the **Tab** key.
- **This step is irreversible.**

  Press **Y**.

The following is displayed:

```
!MCSESM >enable
!*MCSESM #serviceshell deactivate
Notice: If you continue, then the Service Shell is permanently
deactivated.
This step is irreversible!
For details, refer to the Configuration Manual.
Are you sure (Y/N) ?
```

System Monitor 1

The System Monitor 1 provides functions for recovering the operating settings of the switch. If the option of accessing System Monitor 1 during system startup is active, see the **Diagnostics > System > Selftest** dialog, you can start the System Monitor 1 during system startup. The prerequisite is that the PC is connected to the switch through the serial connection.

In System Monitor 1, you carry out the following tasks, for example:

- Managing the operating system and verifying the switch software image
- Starting the operating system
- Deleting configuration profiles, resetting the switch to the factory settings
- Checking boot code information

System Requirements

To access the device management, connect a PC with VT100 terminal emulator to the USB-C interface of the switch.

The following table presents the VT100 terminal emulator settings:

VT100 terminal emulator settings	
Speed	**9600 bit/s**
Data	**8 bit**
Stopbit	**1 bit**
Parity	**None**
Handshake	**None**

Access to Device Management

During system startup, the serial connection to the switch is unavailable through the USB-C interface.

To change to System Monitor 1, perform the following steps:

- Putting the Switch Into Recovery Mode, page 34
- Changing to System Monitor 1, page 34

Putting the Switch Into Recovery Mode

Required accessories:

- External memory (MCSEAM0100)
- USB-C to USB-A adapter (only when you use an external memory device other than the Schneider Electric reference)

Perform the following steps:

- Plug the external memory into the PC.
- Create an empty file recovery.txt in the root directory of the external memory.
- Plug the external memory into the switch.
- Restart the switch.
- Observe the LEDs while the switch boots. When the ***Status*** LED flashes alternately red and green, the switch has successfully booted into the Recovery Mode.

  NOTE: For descriptions of the display elements, refer to the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*.
- Remove the external memory from the switch.

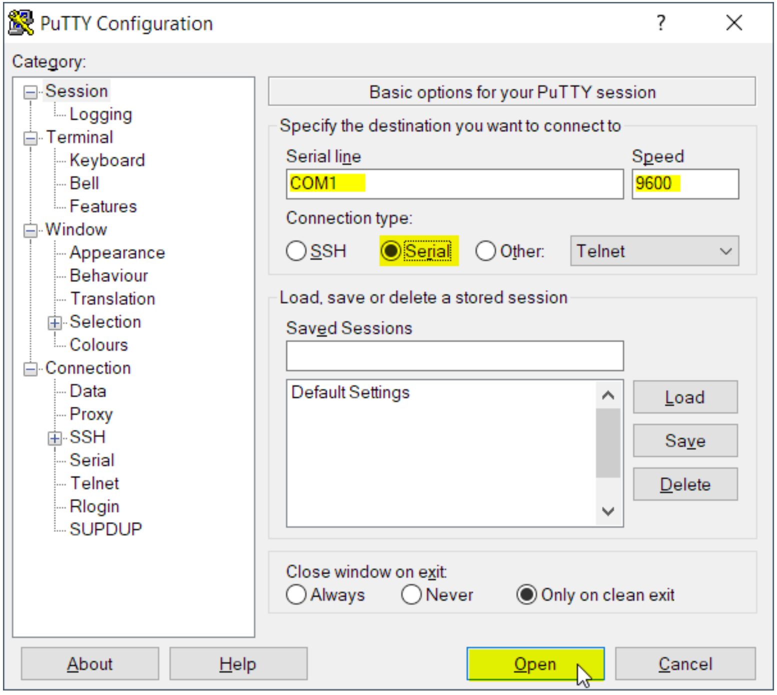
Changing to System Monitor 1

Required accessories:

- USB cable to connect the PC to the USB-C interface of the switch
- PC with VT100 terminal emulator

Perform the following steps:

- Connect the PC to the switch using the USB cable.
- On the PC, start the VT100 terminal emulator.
- Set up the serial connection, then click **Open**.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM1

Speed: 9600

Connection type: ○ SSH ● Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

When the PC and the switch are successfully connected, you see a blank screen.

- Press the **Enter** key.

  After a few seconds, the VT100 terminal emulator displays the System Monitor 1 view:

```
   System Monitor 1
   (Selected OS: ...-99.9_p5-oem-001 (2025-09-20 06:33))
   1  Manage operating system
   3  Start selected operating system
   4  Manage configurations
   5  Show boot code information
   q  End (reset and reboot)
sysMon1>
```

- Select a menu item by entering the number.
- To leave a submenu and return to the main menu, press the **ESC** key.

NOTE: If you intend to leave the external memory permanently plugged in to the switch, first delete the file recovery.txt from the root directory of the external memory.

Replacing a Switch

The device provides the following plug-and-play solutions for replacing a device with a device of the same type:

- The new device loads the configuration profile of the replaced device from the external memory.

  For details, refer to Loading the Configuration Profile from the External Memory, page 92
- The new device gets its IP address using DHCP *Option 82*.

  For details, refer to DHCP L2 Relay, page 327

  For details, refer to Setting Up a DHCP Server With Option 82, page 377

The new device gets the same IP settings that the replaced device had.

- For accessing device management using HTTPS, the device uses a digital certificate. You have the option to transfer your own digital certificate onto the device.

  For details, refer to HTTPS Certificate Management, page 380
- For accessing device management using SSH, the device uses an RSA host key. You have the option to import your own host key in PEM format to the device.

  For details, refer to Transferring an Externally Generated Private RSA Key to the Switch, page 117

Specifying the IP Parameters

When you install the switch for the first time, specify the IP parameters.

The switch provides the following options for entering the IP parameters during the first installation:

- **Command Line Interface:** When you preconfigure your switch outside its operating environment, or restore the network access (In-Band) to the switch, choose this Out-of-Band method.
- **Ethernet Switch Configurator Protocol:** When you have a previously installed network switch or you have another Ethernet connection between your PC and the switch, choose this In-Band method.
- **External Memory:** When you are replacing a switch with one of the same type and have already saved the configuration in the external memory, you choose this method.
- **BOOTP:** To set up the installed switch to use BOOTP, you choose this In-Band method. You need a BOOTP server for this method. The BOOTP server assigns the configuration data to the switch using the MAC address of the switch. The DHCP mode is the default mode for the configuration data reference.
- **DHCP:** To set up the installed switch to use DHCP, you choose this In-Band method. You need a DHCP server for this method. The DHCP server assigns the configuration data to the switch using the MAC address or the system name of the switch.
- **Graphical User Interface:** When the switch has an IP address and is reachable using the network, the Graphical User Interface provides you with another option for configuring the IP parameters.

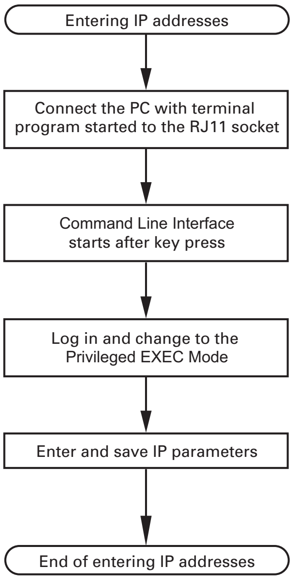
Specifying the IP Parameters Using the Command Line Interface

IPv4

You can configure IP parameters using one of the following methods:

- BOOTP/DHCP
- Ethernet Switch Configurator protocol
- External memory
- Command Line Interface using the serial connection

This flowchart presents the process for entering IP addresses:

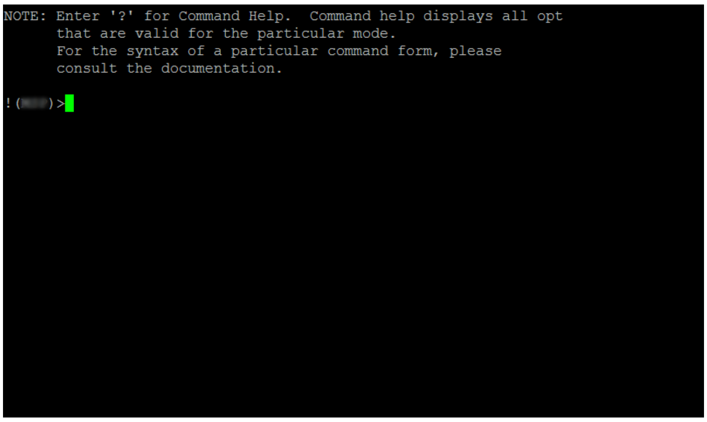

Entering IP addresses
Connect the PC with terminal program started to the RJ11 socket
Command Line Interface starts after key press
Log in and change to the Privileged EXEC Mode
Enter and save IP parameters
End of entering IP addresses

NOTE: If a terminal or PC with terminal emulator is unavailable at the installation site, you can configure the switch at your own workstation, then move it to its final installation location.

Steps to Configure IP Parameters with Command Line Interface:

- Establish a connection to the switch.

  The start screen appears:

```
NOTE: Enter '?' for Command Help.  Command help displays all opt
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

!([redacted])>
```

- Deactivate DHCP (see table below).
- Enter the IP parameters.
  - ◦ Local IP address

    In the default setting, the local IP address is `0.0.0.0`.
  - ◦ Netmask

    Enter the subnet mask if the network is divided into subnets. Default: `0.0.0.0`.
  - ◦ Gateway IP address

    Required only if the switch and the network PC or TFTP server are located in different subnets. Refer to How to Use the Netmask.

    Specify the IP address of the gateway between the subnet with the switch and the path to the network PC.

    In the default setting, the IP address is **0.0.0.0**.
- Save the configuration specified using `copy config running-config nvm`.

The following table presents the description of available commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`network protocol none`	To deactivate DHCP.
`network parms 10.0.1.23 255.255.255.0`	To assign the switch the IP address `10.0.1.23` and the netmask `255.255.255.0`. You have the option of also assigning a gateway address.
`copy config running-config nvm`	To save the updated settings in the non-volatile memory (**NVM**) in the **Selected** configuration profile.

After entering the IP parameters, you can set up the switch using the Graphical User Interface.

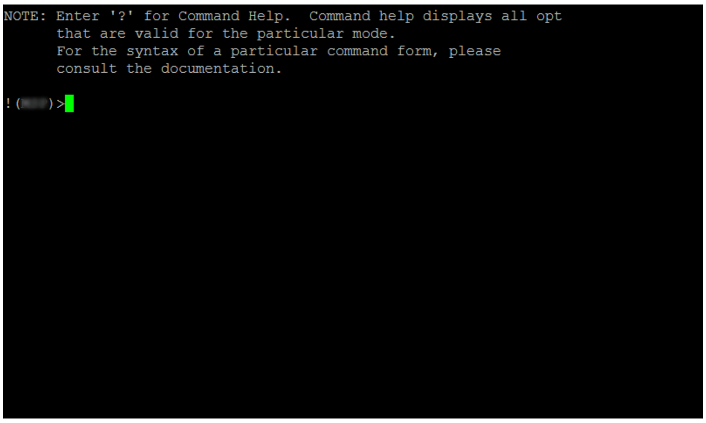
IPv6

The switch allows IPv6 parameters to use the Command Line Interface through the serial connection. Another option to access the Command Line Interface is using a SSH connection with the use of the IPv4 management address.

Perform the following steps:

- Establish a connection to the switch.

  The start screen appears.

  ```
  NOTE: Enter '?' for Command Help.  Command help displays all opt
        that are valid for the particular mode.
        For the syntax of a particular command form, please
        consult the documentation.

  !([redacted])>
  ```

- Enable the IPv6 protocol if the protocol is disabled (see table below).
- Enter the IPv6 parameters.
  - IPv6 address

    The IPv6 address is displayed in a compressed format.
  - Prefix length

    IPv6 uses a prefix length instead of a subnet mask to define the network portion of the address. This role is performed in IPv6 by the prefix length.
  - EUI option function

    You can use the EUI option function to automatically specify the Interface ID of the IPv6 address. The switch uses the MAC address of its interface with the values `ff` and `fe` added between byte 3 and byte 4 to generate a 64 bit Interface ID.

    You can only select this option for IPv6 addresses that have a prefix length equal to 64.
  - IPv6 gateway address

    The IPv6 gateway address is the address of a router through which the switch accesses other switches outside its own network.

    You can specify any IPv6 address except loopback and multicast addresses.

    In the default setting, the IPv6 gateway address is **::**

The following table presents the description of available commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`network ipv6 operation`	To enable the IPv6 protocol if the protocol is disabled. In the default setting, the IPv6 protocol is enabled.
`network ipv6 address add 2001::1 64 eui-64`	To assign the IPv6 address `2001::1` and the prefix length `64`. The `eui-64` parameter is optional. You have the option of also assigning a gateway address.
`copy config running-config nvm`	To save the updated settings in the non-volatile memory (**NVM**) in the **Selected** configuration profile.

After entering the IPv6 parameters, you can set up the switch using the Graphical User Interface. To use an IPv6 address in a URL, use the following URL syntax: **https://[<ipv6_address>]**.

Specifying the IP Parameters Using Ethernet Switch Configurator

The Ethernet Switch Configurator protocol allows IP parameters to be assigned to the switch using Ethernet.

You can set up other parameters using the Graphical User Interface.

Perform the following steps:

- Start the Ethernet Switch Configurator program.

  When Ethernet Switch Configurator is started, Ethernet Switch Configurator automatically searches the network for those switches which support the Ethernet Switch Configurator protocol.

  Ethernet Switch Configurator uses the first network interface found for the PC. When your computer has several network interfaces, you can select the desired network interface in the Ethernet Switch Configurator toolbar.

  Ethernet Switch Configurator displays a line for every switch that responds to a Ethernet Switch Configurator protocol inquiry.

- Identify the displayed switches in the Ethernet Switch Configurator:
  - Select a device line.
  - To set the LEDs to flashing for the selected device, click **Signal** on the tool bar. To stop the flashing, click **Signal** again.
  - By double-clicking a line, you open a window in which you specify the device name and the IP parameter.

  NOTE: Disable the Ethernet Switch Configurator function in the device, after you have assigned the IP parameters to the device.

  NOTE: Save the settings to retain your entries after a restart.

Specifying the IP Parameters Using the Graphical User Interface

IPv4

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Network > Global**. In this dialog, you specify the VLAN in which the device management can be accessed and set up the Ethernet Switch Configurator access.
2	In the VLAN ID column you specify the VLAN in which the device management can be accessed over the network. Note here that you can only access the device management using ports that are members of the relevant VLAN. The **MAC address** field displays the MAC address of the device with which you access the device over the network.
3	In the Ethernet Switch Configurator protocol v1/v2 frame you specify the settings for accessing the device using the Ethernet Switch Configurator software.
4	The Ethernet Switch Configurator protocol allows an IP address to be allocated to the device on the basis of its MAC address. Activate the Ethernet Switch Configurator protocol if you want to allocate an IP address to the device from your PC with the Ethernet Switch Configurator software.
5	Navigate to **Basic Settings > Network > IPv4**. In this dialog, you specify the source from which the device gets its IP parameters after starting.
6	In the Management interface frame you first specify where the device gets its IP parameters from: • In the **BOOTP** mode, the configuration is using a BOOTP or DHCP server on the basis of the MAC address of the device. • In the **DHCP** mode, the configuration is using a DHCP server on the basis of the MAC address or the name of the device. • In the **Local** mode, the device uses the network parameters from the internal device memory. **NOTE:** When you change the allocation mode of the IP address, the device activates the new mode immediately after you click the ✓ button.
7	If required, you enter the IP address, the netmask and the gateway in the IP parameter frame.
8	To apply the settings, click the ✓ button.

IPv6

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Network > IPv6**.
2	The IPv6 protocol is enabled by default. Verify if the **On** radio button is selected in the Operation frame.
3	In the Configuration frame you specify where the device gets its IPv6 parameters from: • If the None radio button is selected, the device receives its IPv6 parameters manually. You can manually specify a maximum number of 4 IPv6 addresses. You cannot specify loopback, link-local, and multicast addresses as static IPv6 addresses. • If the **Auto** radio button is selected, the device receives its IPv6 parameters dynamically with, for example, the use of a Router Advertisement Daemon (radvd). The device receives a maximum of 2 IPv6 addresses. • If the DHCPv6 radio button is selected, the device receives its IPv6 parameters from a DHCPv6 server. The device can receive only one IPv6 address from the DHCPv6 server. • If the All radio button is selected, the device receives its IPv6 parameters using every alternative for both dynamic and manual assignments. **NOTE:** When you change the allocation mode of the IPv6 address, the device activates the new mode immediately after you click the ✓ button.
4	If necessary, you enter the gateway address in the IP parameter frame. **NOTE:** If the **Auto** radio button is selected and you use a Router Advertisement Daemon (radvd), the device automatically receives a link-local type gateway address with a greater metric than the manually set gateway address.
5	In the **Duplicate Address Detection** frame you can specify the number of consecutive *Neighbor Solicitation* messages that the device sends for the **Duplicate Address Detection** Function, page 46.
6	To apply the settings, click the ✓ button.

Manually specify an IPv6 address. To do this, perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Network > IPv6**.
2	Click the + button. The dialog displays the Create window: • Enter the IPv6 address in the **IP address** field. • Enter the IPv6 address prefix length in the **PrefixLength** field. • Click **OK**. The device adds a table row.

Specifying the IP Parameters Using BOOTP

With the **BOOTP** function activated the device sends a boot request message to the BOOTP server. The boot request message contains the Client ID specified in the **Basic Settings > Network > IPv4** dialog. The BOOTP server enters the Client

ID into a database and assigns an IP address. The server answers with a boot reply message. The boot reply message contains the assigned IP address.

Specifying the IP Parameters Using DHCP

IPv4

The Dynamic Host Configuration Protocol (DHCP) is a further development of BOOTP, which it has replaced. The DHCP additionally allows the configuration of a DHCP client using a name instead of using the MAC address.

For the DHCP, this name is *Client Identifier* in accordance with RFC 2131.

The device uses the name entered under *sysName* in the system group of the MIB II as the *Client Identifier*. You can change the system name using the Graphical User Interface (see dialog **Basic Settings > System**), the Command Line Interface or SNMP.

The device sends its system name to the DHCP server. The DHCP server then uses the system name to allocate an IP address as an alternative to the MAC address.

In addition to the IP address, the DHCP server sends:

- Netmask
- Default gateway (if available)
- TFTP URL of the configuration file (if available).

The device applies the configuration data to the appropriate parameters. When the DHCP Sever assigns the IP address, the device permanently saves the configuration data in non-volatile memory (**NVM**).

The following table presents DHCP options which the device requests:

Options	Description
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Hostname
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

The advantage of using DHCP instead of BOOTP is that the DHCP server can restrict the validity of the configuration parameters (“Lease”) to a specific time period (dynamic address allocation). Before this period (“Lease Duration”) elapses, the DHCP client can attempt to renew this lease. As an alternative, the client can negotiate a new lease. The DHCP server then allocates a random free address.

To help avoid this, DHCP servers provide the explicit configuration option of assigning a specific client the same IP address based on a unique hardware ID (static address assignment).

In the default setting, DHCP is activated. As long as DHCP is active, the device attempts to obtain an IP address. When the device cannot find a DHCP server after restarting, it will not have an IP address. The **Basic Settings > Network > IPv4** dialog allows DHCP to be activated or deactivated.

> **NOTE:** When using ConneXium Network Manager network management, verify that DHCP allocates the original IP address to every device.

The appendix contains an example configuration of the BOOTP/DHCP-server.

Example of a DHCP-configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Lines beginning with the # character, contain comments.

The lines preceding the individually listed devices refer to settings that apply to the following device.

The fixed-address line assigns a permanent IP address to the device.

For further information, see the DHCP server manual.

IPv6

The Dynamic Host Configuration Protocol version 6 (DHCPv6) is a network protocol that is used to dynamically specify IPv6 addresses. This protocol is the IPv6 equivalent of the Dynamic Host Configuration Protocol (DHCP) for IPv4. DHCPv6 is described in RFC 8415.

The device uses a DHCP Unique Identifier (DUID) to send a request to the DHCPv6 server. In the device, the DUID represents the Client ID that the DHCPv6 server uses to identify the device that requested an IPv6 address.

The Client ID is displayed in **Basic Settings > Network > IPv6**, in the DHCP frame.

The device can receive only one IPv6 address from the DHCPv6 server, with a PrefixLength of **128**. No gateway address information is provided. If needed, you can manually specify gateway address information.

In the default setting, DHCPv6 protocol is deactivated. You can activate or deactivate the protocol in **Basic Settings > Network > IPv6**. Verify that the DHCPv6 radio button is selected in the Configuration frame.

If you want to dynamically get an IPv6 address with a PrefixLength other than **128**, select the **Auto** radio button. An example here is the use of a Router Advertisement Daemon (radvd). The radvd uses *Router Solicitation* and *Router Advertisement* messages to automatically set up an IPv6 address.

In the default setting, the **Auto** radio button is selected. You can select or clear the **Auto** radio button in the **Basic Settings > Network > IPv6** dialog, in the Configuration frame.

If the All radio button is selected, the device receives its IPv6 parameters using every alternative for both dynamic and manual assignments.

Management Address Conflict Detection

You assign an IP address to the device using several different methods. This function helps the device detect IP address conflicts on a network after the system startup and the device also verifies periodically during operation. This function is described in RFC 5227.

When enabled, the device sends an SNMP trap informing you that it detected an IP address conflict.

The following list contains the default settings for this function:

- Operation: **On**
- Detection mode: **active and passive**
- Send periodic ARP probes: **selected**
- Detection delay [ms]: **200**
- Release delay [s]: **15**
- Address protections: **3**
- Protection interval [ms]: **200**
- Send trap: **selected**

Active and Passive Detection

Actively verifying the network helps prevent the device from connecting to the network with a duplicate IP address. After connecting the device to a network or after configuring the IP address, the device immediately verifies if its IP address exists within the network. To verify the network for address conflicts, the device sends 4 ARP probes with the detection delay of 200 ms into the network. When the IP address exists, the device attempts to return to the previous configuration, and make another verification after the specified release delay time.

When you disable active detection, the device sends two ARP announcements in two-second intervals. Using the ARP announcements with passive detection enabled, the device polls the network to determine if there is an address conflict. If 10 conflicts occur and the release delay interval is less than 60 seconds, the device automatically increases the interval to 60 seconds.

After the device performs active detection or you disable the active detection function, with passive detection enabled the device listens on the network for other devices using the same IP address. When the device detects a duplicate IP address, it initially defends its address by employing the ACD mechanism in the passive detection mode and sends out gratuitous ARPs. The number of protections that the device sends and the protection interval are configurable. To resolve conflicts, if the remote device remains connected to the network, the network interface of the local device disconnects from the network.

When a DHCP server assigns an IP address to the device and an address conflict occurs, the device returns a DHCP decline message.

The device uses the ARP probe method. This has the following advantages:

- ARP caches on other devices remain unchanged
- The method is robust through multiple ARP probe transmissions

Duplicate Address Detection Function

The **Duplicate Address Detection** function determines the uniqueness of an IPv6 unicast address on an interface. The function is performed when an IPv6 address is set up manually, using the DHCPv6, or Auto configuration. The function is also triggered by a change in a link status, for example, a link status change from down to up.

The **Duplicate Address Detection** function uses *Neighbor Solicitation* and *Neighbor Advertisement* messages. You can configure the number of consecutive *Neighbor Solicitation* messages that the device sends. To do this, perform the following steps:

Step	Action
1	Navigate to **Basic Settings** > **Network** > **IPv6**.
2	In the **Duplicate Address Detection** frame, enter the required value in the **Number of neighbor solicitants** field. Possible values: • **0**: The function is disabled. • **1..5**: Default setting is **1**.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`network ipv6 dad-transmits <0..5>`	To set the number of *Neighbor Solicitation* messages that the device sends. The value **0** disables the function.

NOTE: If the **Duplicate Address Detection** function discovers that an IPv6 address is not unique on a link, the device does not log this event in the System Log.

Access to the Switch

First Login (Password Change)

To help prevent unauthorized access to the device, it is imperative that you change the default password during initial setup.

Perform the following steps:

- Open the Graphical User Interface, the Schneider Electric Viewer application, or the Command Line Interface the first time you log into the device management.
- Log into the device management with the default password.

  The device prompts you to type in a new password.
- Type in your new password.

  Choose a password that contains at least 8 characters which includes uppercase characters, lowercase characters, numerical digits, and special characters.
- When you log into the device management through the Command Line Interface, the device prompts you to confirm your new password.
- Log into the device management again with your new password.

NOTE: If you lost your password, contact your local support team.

Authentication Lists

When a user accesses the device management using a defined connection type, the device verifies the login credentials of the user through an authentication list which contains the policies that the device applies for authentication.

The prerequisite for a user to access the device management is that at least one policy is assigned to the authentication list of the application through which access is performed.

Applications

The device provides an application for each type of connection through which you access the device:

- Access to the Command Line Interface using the serial connection: **Console (V.24)**
- Access to the Command Line Interface using SSH: **SSH**
- Access to the Command Line Interface using Telnet: **Telnet**
- Access to the Graphical User Interface: **WebInterface**

The device also provides an application to control the access to the network from connected end devices using port-based access control: **8021x**.

Policies

When a user logs in with valid login data, the device grants access to its device management interface. The device authenticates the users using the following policies:

- User management of the device
- LDAP

- RADIUS
- TACACS+

When the end device logs in with valid login data, the device gives the connected end devices access to the network with the port-based access control according to IEEE 802.1X. The device authenticates the end devices using the following policies:

- RADIUS
- IAS (Integrated Authentication Server)
- TACACS+

The device gives you the option of a fallback solution. For this, you specify more than one policy in the authentication list. When authentication is unsuccessful using the up-to-date policy, the device applies the next specified policy.

Managing Authentication Lists

You manage the authentication lists in the Graphical User Interface or in the Command Line Interface. To do this, perform the following steps:

Step	Action
1	Navigate to **Device Security > Authentication List**. The dialog displays the authentication lists that are set up. To display the authentication lists that are set up, execute the following command: `show authlists`
2	Deactivate the authentication list that is not used for device access (for example **8021x**): • In the Active column of the authentication list **defaultDot1x8021AuthList**, clear the checkbox. • To apply the settings, click the ✓ button. To deactivate the authentication list **defaultDot1x8021AuthList**, execute the following command: `authlists disable defaultDot1x8021AuthList`

Adjusting the Settings

Example: Set up a separate authentication list for the application **WebInterface** which is by default included in the authentication list **defaultLoginAuthList**.

The device passes authentication requests to a RADIUS or TACACS+ server in the network. As a fallback solution, the device authenticates users using the local user management. To do this, perform the following steps:

Step	Action
1	Create the authentication list **loginGUI**: • Navigate to **Device Security > Authentication List**. • Click the ⊞ button. The dialog displays the Create window. ◦ Enter a meaningful name in the **Name** field. In this example, enter the name **loginGUI**. ◦ Click **OK**. The device adds a table row. Execute the following commands: • `enable`: To change to the Privileged EXEC mode. • `configure`: To change to the Configuration mode. • `authlists add loginGUI`: To add the authentication list **loginGUI**.
2	Select the policies for the authentication list **loginGUI**: • In the Policy 1 column, select the value **radius**. • In the Policy 2 column, select the value **local**. • In the Policy 3 to Policy 5 columns, select the value **reject** to help prevent further fallback. • To apply the settings, click the ✓ button. Execute the following commands: • `authlists set-policy loginGUI radius local reject reject reject`: To assign the policies **radius**, **local** and **reject** to the authentication list **loginGUI**. • `show authlists`: To display the authentication lists that are set up.
3	Assign an application to the authentication list **loginGUI**: • Navigate to **Device Security > Authentication List**. • In the table, select the authentication list **loginGUI**. • Click the 📋 button. The dialog displays the Allocate applications window. • Click the application **WebInterface** to highlight it. • Click **OK**. The dialog displays the updated settings: ◦ The Dedicated applications column of authentication list **loginGUI** displays the application **WebInterface**. ◦ The Dedicated applications column of authentication list **defaultLoginAuthList** does not display the application **WebInterface** anymore. • To apply the settings, click the ✓ button. Execute the following commands: • `show appllists`: To display the applications and the allocated lists. • `appllists set-authlist WebInterface loginGUI`: To assign the **loginGUI** application to the authentication list **WebInterface**.

User Management

When a user logs in with valid login data, the device grants access to its device management interface. The device authenticates the user either using the local user management or with a RADIUS or TACACS+ server in the network. To get the device to use the user management, assign the **local** policy to an authentication list, see the **Device Security > Authentication List** dialog.

In the local user management, you manage the user accounts. One user account is usually allocated to each user.

Access Roles

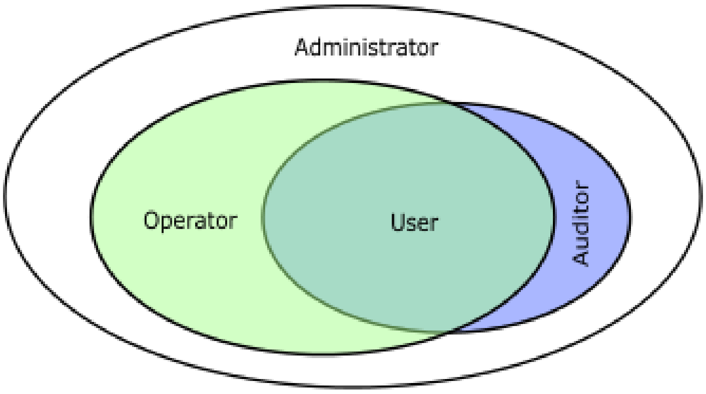
The device allows a role-based authorization model to specifically control the access to the device management. Users to whom a specific authorization profile is allocated can use commands and functions from the same authorization profile or a lower one.

The device uses the authorization profiles on every application with which the device management can be accessed.

> **NOTE:** The following applies to the Command Line Interface: Users to whom a specific authorization profile is assigned can use commands and functions from this authorization profile or a lower level role. The commands available to a user also depend on the Command Line Interface mode in which the user is working. See Mode-Based Command Hierarchy, page 22.

Every user account is linked to an access role that regulates the access to the individual functions of the device. Depending on the planned activity for the respective user, you assign a pre-defined access role to the user.

The device differentiates between the following access roles:



The following table presents access roles for user accounts

Role	Description	Authorized for the following activities
administrator	The user is authorized to monitor and administer the device.	All activities with read/write access, including the following activities reserved for an administrator: • Add, modify or delete user accounts • Activate, deactivate or unlock user accounts • Change every password • Set up the password management • Set or change system time • Load files to the device, for example, device settings, certificates, or device software images • Reset settings and security-related settings to the state on delivery • Set up the RADIUS or TACACS+ server and the authentication lists • Apply scripts using the Command Line Interface • Enable/disable CLI logging and SNMP logging • External memory activation and deactivation • Activate or deactivate System Monitor 1 • Enable/disable the services for the access to the device management (for example SNMP). • Set up access restrictions to the Graphical User Interface or the Command Line Interface based on the IP addresses
operator	The user is authorized to monitor and set up the device, with the exception of security-related settings.	All activities with read/write access, with the exception of the previously-named activities, which are reserved for an administrator:
auditor	The user is authorized to monitor the device and to save the log file in the **Diagnostics > Report > Audit Trail** dialog.	Monitoring activities with read access.
guest	The user is authorized to monitor the device - with the exception of security-related settings.	Monitoring activities with read access.
unauthorized	No access to the device possible. • As an administrator you assign this access role to temporarily lock a user account. • If an administrator assigns a different access role to the user account and an error is detected, the device assigns this access role to the user account.	No activities permitted.

Managing User Accounts

You manage the user accounts in the Graphical User Interface or in the Command Line Interface. To do this, perform the following step:

- Navigate to **Device Security > User Management**.

  The dialog displays the user accounts that are set up.

Execute the following command:

- `show users`: To display the user accounts that are set up.

Default User Accounts

In the default setting, the user account **admin** is set up in the device as follows:

Parameter	Default setting
User name	**admin**
Password	**private**
Role	**administrator**
User locked	**cleared**
Policy check	**cleared**
SNMP auth type	**hmacmd5**
SNMP encryption type	**des**

Change the password for the **admin** user account before making the device available in the network.

Changing Default Passwords

To help prevent unauthorized access, change the password of the default user account. To do this, perform the following steps in order to change the password for the **admin** user account:

Step	Action
1	Navigate to **Device Security > User Management**. The dialog displays the user accounts that are set up.
2	To require a specified minimum complexity for the passwords, select the checkbox in the Policy check column. Before saving it, the device verifies the password according to the policy specified in the Password policy frame. **NOTE:** The password verification can lead to a message in the Security status frame in **Basic Settings > System**. You specify the settings that cause this message in **Basic Settings > System**.
3	Click the table row of the relevant user account in the **Password** field. Enter a password of at least 6 characters. Up to 64 alphanumeric characters are permitted: • The device differentiates between upper and lowercase. • The minimum length of the password is specified in the Configuration frame. The device constantly verifies the minimum length of the password.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users password-policy-check <user> enable`	To activate the verification of the password for the **<user>** user account based on the specified policy. In this way, you require a specified minimum complexity for the passwords.
`users password USER SECRET`	To specify the password **SECRET** for the user account **USER**. Enter at least 6 characters.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

NOTE: When you display the security status, the password verification can lead to a message (`show security-status all`). You specify the settings that cause this message with the command `security-status monitor pwd-policy-inactive`.

Setting Up a New User Account

Allocate a separate user account to each user that accesses the device management. In this way you can specifically control the authorizations for the access.

In the following example, you set up the user account for a user **USER** with the access role **operator**. Users with the access role **operator** are authorized to monitor and set up the device, with the exception of security-related settings.

To create a user account, perform the following steps:

Step	Action
1	Navigate to **Device Security > User Management**.
2	Click the ⊞ button. The dialog displays the Create window.
3	Enter the name in the **User name** field. In this example, you give the user account the name **USER**.
4	Click **OK**.
5	To require a specified minimum complexity for the passwords, select the checkbox in the Policy check column. Before saving it, the device verifies the password according to the policy specified in the Password policy frame.
6	In the **Password** field, enter a password of at least 6 characters. Up to 64 alphanumeric characters are permitted. • The device differentiates between upper and lowercase. • The minimum length of the password is specified in the Configuration frame. The device constantly verifies the minimum length of the password.
7	In the Role column, select the access role. In this example, you select the value **operator**.
8	To activate the user account, select the checkbox in the Active column.
9	To apply the settings, click the ✓ button. The dialog displays the user accounts that are set up.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users add USER`	To add the **USER** user account.
`users password-policy-check USER enable`	To activate the verification of the password for the **USER** user account based on the specified policy. In this way, you require a specified minimum complexity for the passwords.
`users password USER SECRET`	To specify the password **SECRET** for the user account **USER**. Enter at least 6 characters.
`users access-role USER operator`	To assign the access role **operator** to the user account **USER**.
`users enable USER`	To activate the user account **USER**.
`show users`	To display the user accounts that are set up.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

NOTE: When you are setting up a new user account in the Command Line Interface, allocate the password.

Deactivating the User Account

When a user account is deactivated, the device prevents that user from accessing to device management. Deactivation retains the user account configuration data, whereas deleting the account removes it permanently.

To temporarily deactivate the user account in order to keep the user account settings and reuse them in the future, perform the following steps:

Step	Action
1	Navigate to **Device Security > User Management**. The dialog displays the user accounts that are set up.
2	In the table row for the relevant user account, clear the checkbox in the Active column.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users disable <user>`	To disable user account.
`show users`	To display the user accounts that are set up.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

To permanently deactivate the user account settings and to delete the user account, perform the following steps:

Step	Action
1	Select the table row of the relevant user account.
2	Click the ✖ button.

Execute the following commands:

Command	Description
`users delete <user>`	To delete the user account **<user>**.
`show users`	To display the user accounts that are set up.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Adjusting Policies for Passwords

The device verifies each password against the configured password policy. Enforcing this policy ensures that all passwords meet the required complexity. Password-policy enforcement can be enabled or disabled individually for each user account. If the checkbox is selected and the new password complies with the policy, the device accepts the password change.

In the default settings, practical values for the policy are set up in the device. You have the option of adjusting the policy for passwords to meet your requirements. To do this, perform the following steps:

Step	Action
1	Navigate to **Device Security > User Management**.
2	In the Configuration frame you specify the number of consecutive unsuccessful login attempts before the device locks out the user. You also specify the minimum number of characters that defines a password. **NOTE:** Only users with **administrator** authorization can remove the lock. The number of consecutive unsuccessful login attempts as well as the possible lockout of the user apply only when accessing device management through: • Graphical User Interface • SSH protocol • Telnet protocol **NOTE:** When accessing device management using the Command Line Interface through the serial connection, the number of unsuccessful login attempts is unlimited.
3	Specify the values to meet your requirements: • In the **Login attempts** field you define the number of times a user may attempt to log in to the device management. Values in the range **0..5** are permitted. In the previous example, the value **0** deactivates the function. • In the **Min. password length** field, you define the minimum allowed password length. Values in the range **1..64** are permitted. The dialog displays the policy set up in the Password policy frame.
4	Adjust the values to meet your requirements. Values in the range **1** through **16** are permitted. The value **0** deactivates the relevant policy.
5	To apply the entries specified in the Configuration and Password policy frames, select the checkbox in the Policy check column for a particular user.
6	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`passwords min-length 6`	To specify the policy for the minimum length of the password.
`passwords min-lowercase-chars 1`	To specify the policy for the minimum number of lowercase letters in the password.
`passwords min-numeric-chars 1`	To specify the policy for the minimum number of digits in the password.
`passwords min-special-chars 1`	To specify the policy for the minimum number of special characters in the password.
`passwords min-uppercase-chars 1`	To specify the policy for the minimum number of uppercase letters in the password.
`show passwords`	To display the policies that are set up.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

LDAP Function

Server administrators manage *Active Directories* which contain user login credentials for applications used in the office environment. The *Active Directory* is hierarchical in nature, containing user names, passwords, and the authorized read/write permission levels for each user.

This device uses the Lightweight Directory Access Protocol (LDAP) to retrieve user login information and permission levels from an *Active Directory*. This enables a single sign-on for network devices. When login credentials are retrieved from an *Active Directory*, users can authenticate with the same credentials they use in their office environment.

An LDAP session starts with the device contacting the Directory System Agent (DSA) to search the *Active Directory* of an LDAP server. If the server finds multiple entries in the *Active Directory* for a user, the server sends the greater permission level found. The DSA listens for information requests and sends responses on TCP port **389** for LDAP, or on TCP port **636** for LDAP over SSL (LDAPS). Clients and servers encode LDAPS requests and responses using the Basic Encoding Rules (BER). The device opens a new connection for every request and closes the connection after receiving a response from the server.

The device allows the transfer of a digital certificate to the device. The certificate helps the device to verify the server for Secure Socket Layer (SSL) and Transport Layer Security (TLS) connections. Use only digital certificates signed by a Certification Authority (CA).

The device allows up to four authentication servers. An authentication server authenticates and authorizes the user when the device forwards the login data to the server.

The device can cache login credentials for up to 1024 users in memory. If the active directory servers are unreachable, the users are still able to log in using their office login credentials.

Coordination with the Server Administrator

Configuring the LDAP function requires that the network administrator request the following information from the server administrator:

- The server name or IP address
- The location of the *Active Directory* on the server
- The type of connection used
- The TCP listening port
- When required, the location of the digital certificate
- The name of the attribute containing the user login name
- The names of the attribute containing the user permission levels

The server administrator can assign permission levels individually using an attribute such as **description**, or to a group using the **memberOf** attribute. In the **Device Security > LDAP > Role Mapping** dialog you specify which attributes receive the various permission levels.

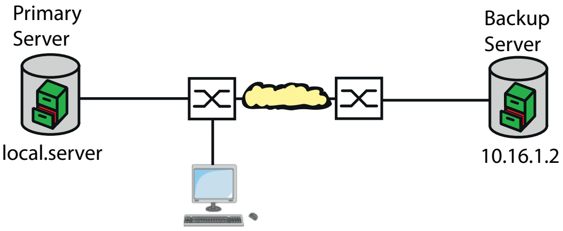
You also have the option to retrieve the name of the attributes containing the user login name and permission levels using a LDAP browser such as JXplorer or Softerra.

Setting Up LDAP

The device can establish an encrypted link to a local server using only the server name or to a server on a different network using an IP address. The server administrator uses attributes to identify login credentials of a user and assign individual and group permission levels.

Using information received from the server administrator, you specify which attributes in the *Active Directory* contain the user login credentials and the permission level. The device then compares the user login credentials with the permission levels specified in the device and allows the user to log into the device management at the assigned permission level.

The following figure presents an example of the LDAP setup:



In this example, the server administrator sent the following information:

Information	Primary Server	Backup Server
The server name or IP address	**local.server**	**10.16.1.2**
The location of the *Active Directory* on the server	**Country/City/User**	**Country/Company/User**
The type of connection used	**TLS** (with digital certificate)	**SSL**
The server administrator sent the digital certificate in an email.	Digital certificate for primary server saved locally	Digital certificate for backup server saved locally
The TCP listening port	**389 (tls)**	**636 (ssl)**
Name of the attribute containing the user name	**userPrincipalName**	**userPrincipalName**
The names of the attribute containing the user permission levels	**OPERATOR** **ADMINISTRATOR**	**OPERATOR** **ADMINISTRATOR**

Perform the following steps:

Step	Action
1	Navigate to **Device Security > Authentication List**.
2	To set up the device to retrieve the user login credentials from the first *Active Directory*, specify for the **defaultLoginAuthList** list the value **ldap** in the Policy 1 column.
3	Navigate to **Device Security > LDAP > Configuration**.
4	The device allows the length of time that it saves the user login credentials in the cache to be specified. To cache user login credentials for a day, in the Configuration frame, **Client cache timeout [min]** field, specify the value **1440**.
5	The Bind user entry is optional. When specified, users enter only their user name to log in. The service user can be anyone with login credentials listed in the *Active Directory* under the attribute specified in the User name attribute column. In the Bind user column, specify the user name and the domain.
6	The Base DN is a combination of the domain component (dc) and the organizational unit (ou). The Base DN allows the device to locate a server in a domain (dc) and find the *Active Directory* (ou). Specify the location of the *Active Directory*. In the Base DN column, specify the value **ou=Users, ou=City,ou=Country,dc=server,dc=local**.
7	In the User name attribute column, enter the value **userPrincipalName** to specify the attribute under which the server administrator lists the users. The device uses a digital certificate to verify the identity of the server:
8	When the file is located on your PC or on a network drive, drag and drop it onto the ↥ area. As an alternative, click in the area to select the file: • To transfer the file to the device, click **Start**. • To add a table row, click the + button. • To specify a description, enter the value **Primary AD Server** in the Description column. • To specify the server name and domain of the primary server, in the Address column, enter the value **local.server**. • The primary server uses the TCP port **389** for communication which is the Destination TCP port default value. • The primary server uses TLS for encrypting communication and a digital certificate for server validation. In the Connection security column, specify the value **startTLS**. • To activate the table row, select the checkbox in the Active column. • Using the information received from the Backup server administrator, add and activate another table row, then specify the settings in the corresponding columns.
9	Navigate to **Device Security > LDAP > Role Mapping**.
10	To add a table row, click the + button.
11	When a user logs into the device management, with LDAP set up and enabled, the device searches the *Active Directory* for the login credentials of the user. If the device finds the user name and the password is correct, the device searches for the value specified in the Type column. If the device finds the attribute and the text in the Parameter column matches the text in the *Active Directory*, the device allows the user to log into the device management with the assigned permission level. When the value **attribute** is specified in the Type column, specify the value in the Parameter column in the following form: **attributeName=attributeValue**.
12	In the Role column, enter the value **operator** to specify the access role.
13	To activate the table row, select the checkbox in the Active column.

Step	Action
14	Click the ⊞ button. The dialog displays the Create window. Enter the values received from the server administrator for the access role **administrator**. To activate the table row, select the checkbox in the Active column.
15	Navigate to **Device Security > LDAP > Configuration**.
16	Enable the LDAP function. Select the **On** radio button in the Operation frame.

The following table describes how to set up the LDAP function in the device using the Command Line Interface. The table displays the commands for Index=**1**. To set up other indexes, use the same commands and substitute the appropriate information:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ldap cache-timeout 1440`	To specify the device to flush the non-volatile memory after a day.
`ldap client server add 1 local.server port 389`	To add a connection to the remote authentication client server with the hostname **local.server** and the UDP port **389**.
`ldap client server modify 1 security startTLS`	To specify the type of security used for the connection.
`ldap client server modify 1 description Primary_AD_Server`	To specify the configuration name of the entry.
`ldap basedn ou=Users,ou=City,ou=Country,dc=server,dc=local`	To specify the Base Domain Name used to find the *Active Directory* on the server.
`ldap search-attr userPrincipalName`	To specify the attribute to search for in the *Active Directory* which contains the login credential of the users.
`ldap bind-user user@company.com`	To specify the name and domain of the service user.
`ldap bind-passwd Ur-123456`	To specify the password of the service user.
`ldap client server enable 1`	To enable the remote authentication client server connection.
`ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR`	To add a remote authentication role mapping entry for the access role **operator**. Map the access role **operator** to the attribute containing the word **OPERATOR**.
`ldap mapping enable 1`	To enable the remote authentication role mapping entry.
`ldap operation`	To enable the remote authentication function.

SNMP Access

The Simple Network Management Protocol (SNMP) allows a network management system to monitor the device over the network and change its settings.

SNMPv1/v2 Access

Using SNMPv1 or SNMPv2 the network management system and the device communicate unencrypted. Every SNMP packet contains the *community name* in plain text and the IP address of the sender.

The *community names* **user** for *read-only* access and **admin** for *read and write* access are preset in the device. If SNMPv1/v2 is enabled, the device allows anyone who knows the *community name* access to the device.

To help prevent unwanted access, perform the following steps:

- Change the default *community names* in the device.

  Treat the *community names* with discretion.

  Anyone who knows the *community name* for write access, has the ability to change the settings of the device.
- Specify a different *community name* for *read and write* access than for *read-only* access.
- Use SNMPv1 or SNMPv2 only in environments protected from eavesdropping. The protocols do not use encryption.
- Deactivate the write access for the SNMPv1/v2 **Write** community.
- Use, if possible, SNMPv3 and disable access using SNMPv1 and SNMPv2 in the device.

SNMPv3 Access

Using SNMPv3 the network management system and the device communicate encrypted. The network management system authenticates itself with the device using the login credentials of a user. The prerequisite for the SNMPv3 access is that in the network management system uses the same settings that are defined in the device.

The device allows the SNMP auth type and SNMP encryption type parameters to be specified individually in each user account.

When you set up a new user account in the device, the parameters are preset so that the network management system ConneXium Network Manager reaches the device immediately.

The user accounts set up in the device use the same passwords in the Graphical User Interface, in the Command Line Interface, and for SNMPv3.

To adapt the SNMPv3 parameters of the user account settings to the settings in the network management system, perform the following steps:

Step	Action
1	Navigate to **Device Security > User Management**. The dialog displays the user accounts that are set up.
2	Click the table row of the relevant user account in the **SNMP auth type** field. Select the desired setting.
3	Click the table row of the relevant user account in the **SNMP encryption type** field. Select the desired setting.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users snmpv3 authentication <user> md5 | sha1`	To assign the HMAC-MD5 or HMACSHA protocol for authentication requests to the user account **<user>**.
`users snmpv3 encryption <user> des | aescfb128 | none`	To assign the DES or AES-128 algorithm to the user account **<user>**. With this algorithm, the device encrypts authentication requests. The value **none** removes the encryption.
`show users`	To display the user accounts that have been set up.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

SNMPv3 Traps

SNMP version 3 allows the device to use encrypted communication with a network management system.

For this, you need to set up the following roles in the device:

- SNMPv3 Trap Users, page 62
- SNMPv3 Trap Hosts, page 63

SNMPv3 Trap Users

An *SNMPv3 trap* user has the permission to send *SNMPv3 traps* to the specified *SNMPv3 trap* hosts.

An *SNMPv3 trap* user is exclusively for sending *SNMPv3 traps* to *SNMPv3 trap* hosts. Do not confuse *SNMPv3 trap* users with device user accounts. For details, refer to Managing User Accounts, page 51.

The device supports encryption and authentication for sending *SNMPv3 traps*. The device allows *SNMPv3 trap* users.

The device supports the following authentication and encryption types:

- `auth-no-priv`

  The user needs to authenticate to send *SNMPv3 traps*. The device sends the *SNMPv3 traps* unencrypted.
- `auth-priv`

  The user needs to authenticate to send *SNMPv3 traps*. The device sends the *SNMPv3 traps* encrypted.
- `no-auth`

  Do not use this setting if you transmit data over untrusted networks.

  The device sends the *SNMPv3 traps* unencrypted without authentication.

To add an *SNMPv3 trap* user, execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp notification user add <name1> auth-priv auth sha1 <passphrase1> priv des <passphrase2>`	To add the *SNMPv3 trap* user **<name1>**: • With authentication and encryption • SNMPv3 authentication parameters • SHA1 as the cryptographic hash function for *SNMPv3 trap* user authentication • **<passphrase1>** as passphrase • SNMPv3 encryption parameters • DES as the *SNMPv3 trap* encryption algorithm • **<passphrase2>** as passphrase.
`show snmp notification users`	To display the *SNMPv3 trap* user settings.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

To modify an existing *SNMPv3 trap* user, delete the user and add a new user with the desired settings.

To delete an *SNMPv3 trap* user, execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp notification user delete <name1>`	To delete the *SNMPv3 trap* user **<name1>**.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

SNMPv3 Trap Hosts

An *SNMPv3 trap* host is the destination for an *SNMPv3 trap* that the device sends.

The device supports a maximum of 10 *SNMP trap* hosts.

To specify an *SNMPv3 trap* host, execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp notification host add <hostname1> a.b.c.d user <name2> auth-priv`	To add the *SNMPv3 trap* host **<hostname1>** • With the IPv4 address **<a.b.c.d>** • Username **<name2>** • With authentication and encryption
`show snmp notification hosts`	To display the *SNMPv3 trap* host settings.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

To modify an existing *SNMPv3 trap* host, delete the host and add a new host with the desired settings.

To delete an *SNMPv3 trap* host, execute the following commands:

Command	**Description**
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp notification host delete <hostname1>`	To delete the *SNMPv3 trap* host **<hostname1>**.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Out-of-Band Access

The device has a separate port that allows access to the device management out-of-band. When there is a high in-band load on the switching ports, you can still use this separate port to access the device management.

The prerequisite is that you connect the PC directly to the USB port. When you use Microsoft Windows, install the RNDIS driver, where necessary. As soon as you connect the PC, it can communicate with the device management over a virtual network connection.

In the default setting, you can access the device management through this port using the following IP parameters:

- IP address: **91.0.0.100**
- Netmask: **255.255.255.0**

The device allows access to the device management using the following protocols:

- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP
- Industry protocols:
  - IEC 61850-MMS
  - Modbus TCP
  - EtherNet/IP

Specifying the IP Parameters

When you connect the PC through the USB port, the device assigns the IP address of the USB network interface, increased by 1, to the PC (**91.0.0.101** in the default setting). The device allows change of the IP parameters to adapt the device to the requirements of your environment.

Verify that the IP subnet of this network interface does not overlap with any subnet connected to another interface of the device:

- Management interface

If the PC accesses the device management through the USB port, the device disconnects the Graphical User Interface and Command Line Interface immediately after you have performed the changes.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Out-of-Band over USB**.
2	Overwrite the IP address in the IP parameter frame, **IP address** field.
3	To apply the settings, click the ✓ button.

Execute the following commands:

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><code>enable</code></td><td>To change to the Privileged EXEC mode.</td></tr>
<tr><td><code>network usb parms 192.168.1.1 255.255.255.0</code></td><td>To specify the IP address <b>192.168.1.1</b> and the netmask <b>255.255.255.0</b> for the USB network interface.</td></tr>
<tr><td><code>show network usb</code></td><td>To display the USB network interface settings.</td></tr>
<tr><td colspan="2"><pre>
Out-of-band USB management settings

Management operation........................enabled
IP address..................................192.168.1.1
Subnet mask.................................255.255.255.0
Host MAC address............................64:60:38:1f:85:85
Device MAC address..........................64:60:38:1f:85:86
</pre></td></tr>
<tr><td><code>save</code></td><td>To save the settings in the non-volatile memory (<b>nvm</b>) in the <b>Selected</b> configuration profile.</td></tr>
</table>

Disabling the USB Network Interface

In the default setting, the USB network interface is enabled. If you do not want someone to access device management through the USB port, the device allows the USB network interface to be disabled.

If the PC accesses the device management through the USB port, the device disconnects the Graphical User Interface and Command Line Interface immediately after you have performed the changes.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Out-of-Band over USB**.
2	Disable the USB network interface. Select the **Off** radio button in the Operation frame.
3	To apply the settings, click the ✓ button.

Execute the following commands:

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>enable</td><td>To change to the Privileged EXEC mode.</td></tr>
<tr><td>no network usb operation</td><td>To disable the USB network interface.</td></tr>
<tr><td colspan="2"><pre>
Out-of-band USB management settings

Management operation........................disabled
IP address..................................192.168.1.1
Subnet mask.................................255.255.255.0
Host MAC address............................64:60:38:1f:85:85
Device MAC address..........................64:60:38:1f:85:86
</pre></td></tr>
<tr><td>save</td><td>To save the settings in the non-volatile memory (<b>nvm</b>) in the <b>Selected</b> configuration profile.</td></tr>
</table>

TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol used for centralized user authentication and authorization. The TACACS+ protocol helps verify the identity of a user who is trying to access a network device. It also supports fine-grained control over which Command Line Interface commands the user is permitted to execute on the device.

Compared to the RADIUS protocol, the TACACS+ protocol helps ensure greater security by encrypting the entire communication.

The prerequisite for using TACACS+ on the device is that a TACACS+ server is available in the network.

The TACACS+ protocol controls access to the device over the following connections:

- Telnet
- SSH
- Serial connection

The TACACS+ protocol has the following benefits for administrators:

- General control over the access role to be assigned to an authenticated user.
- Fine-grained control over the Command Line Interface commands that the user is permitted to execute.

Setting Up a TACACS+ Server on the Switch

To use TACACS+ on the device, set up at least one TACACS+ server. TACACS+ uses the TCP port **49** for communication between the client and the server. You can specify a different port on the device, if necessary.

Perform the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`tacacs server add {<ipv4> | <ipv6> | <dns name>}`	To specify the TACACS+ server address.
`tacacs server modify {<ipv4> | <ipv6> | <dns name>} port <port>`	To modify the TCP port through which the device communicates with the TACACS+ server.

Command	Description
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.
`exit`	To change to the Privileged EXEC mode.

Specifying an Individual TACACS+ Server Key

For encrypted communication between the device and a TACACS+ server, you can specify an individual TACACS+ server key.

Perform the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`tacacs server modify {<ipv4> | <ipv6> | <dns name>} key`	To specify a TACACS+ server key that the device uses for the communication with this specific TACACS + server. Press the **Enter** key.
`Enter key (128 characters max): <key>`	Enter the new key. The maximum length of the key is 128 characters. Press the **Enter** key.
`Re-enter key: <key>`	Re-enter the new key. Press the **Enter** key.
`Key has been changed!`	The individual TACACS+ server key is changed.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.
`exit`	To change to the Privileged EXEC mode.

Specifying a Global TACACS+ Server Key

For encrypted communication between the device and multiple TACACS+ servers, you can specify a global TACACS+ server key. The device will use this key if no key is specified for an individual TACACS+ server.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`tacacs server key`	To specify a TACACS+ server key that the device can use for the communication with multiple TACACS+ servers. Press the **Enter** key.
`Enter key (128 characters max): <key>`	Enter the new key. The maximum length of the key is 128 characters. Press the **Enter** key.
`Re-enter key: <key>`	Re-enter the new key. Press the **Enter** key.
`Key has been changed!`	The global TACACS+ server key is changed.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.
`exit`	To change to the Privileged EXEC mode.

Authenticating Users Through TACACS+

To authenticate users through a TACACS+ server, add the **tacacs** policy to an authentication list. For details, refer to Authentication Lists, page 47.

The device provides you with the following options:

- Adding the **tacacs** policy to a preset authentication list.
- Creating a new authentication list and adding the **tacacs** policy to this authentication list.

During authentication, the TACACS+ server assigns a privilege level to the user, which determines the corresponding access role on the device. Depending on the allocated access role, the user has access to a specific set of commands. This set of commands is preset on the device for each access role. For details, refer to Access Roles, page 50.

In the following example, you set up **tacacs** as the first policy the device uses to authenticate users who log on to the device over the serial connection.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`authlists set-policy defaultV24AuthList tacacs local radius reject reject`	To specify **tacacs** as the first policy of the preset authentication list **defaultV24AuthList**.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.
`exit`	To change to the Privileged EXEC mode.

Authorizing Commands Through TACACS+

If command authorization is disabled, the user has access to the set of commands preset for the access role assigned during authentication. This set of commands is preset on the device for each access role. For details, refer to Access Roles, page 50.

If command authorization is enabled, the device verifies with the TACACS+ server each command that the user wants to execute on the device. The TACACS+ server then confirms whether the user is permitted to execute the respective command.

For already logged-in users, the status of command authorization remains unchanged. Any changes to the status of command authorization take effect only after the user logs out and in again.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`tacacs command-authorization operation`	To enable command authorization.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.
`exit`	To change to the Privileged EXEC mode.

Accounting User Activity on the Switch

The accounting function of the TACACS+ protocol tracks actions performed by authenticated users on the device. The device generates a record for every successful user action. The device immediately sends each generated record to the TACACS+ server in the network. This helps the network administrator or security officers get an overview of the successful user actions performed on network devices.

The device supports the *stop-only* mode of the TACACS+ accounting function. The device tracks user activity, even if the user authenticated through a protocol other than TACACS+.

When you enable the accounting function, the device generates one of the following records when a relevant event occurs:

- *Login record*

  when a user session starts
- *Accounting record*

  for each command successfully executed during a user session
- *Logout record*

  when a user session ends

Security considerations:

- The TACACS+ accounting function does not record unsuccessful login attempts nor attempts to execute disallowed commands.
- The information exchanged between the device and the TACACS+ server is only obfuscated by the TACACS+ protocol, not encrypted. Use the TACACS+ accounting function only if you can accept this level of security.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`tacacs accounting command mode stop-only`	To enable accounting on the device.
`show tacacs global`	To display the status of the accounting function.

`TACACS+ client global settings`
`------------------------------`
`...`
`TACACS+ command accounting mode..............stop-only`	

`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.
`exit`	To change to the Privileged EXEC mode.

Synchronizing the System Time in the Network

Many applications rely on a time that is as correct as possible. The necessary accuracy, and thus the allowable deviation from the actual time, depends on the application area.

Examples of application areas include:

- Log entries
- Time stamping of production data
- Process control

The device allows the synchronization of the time in the network using the following options:

- The Simple Network Time Protocol (SNTP) is a solution for low accuracy requirements. Under ideal conditions, the Simple Network Time Protocol (SNTP) achieves accuracy in the millisecond range. The accuracy depends on the signal delay.
- The Precision Time Protocol (PTP) along with IEEE 1588 achieves accuracy on the order of sub-microseconds. This protocol is suitable for demanding applications up to and including process control.

When the involved devices support the Precision Time Protocol (PTP), it is usually the better choice. The Precision Time Protocol (PTP) is more accurate, has advanced methods of error correction, and causes only a low network load. The implementation of the Precision Time Protocol (PTP) is comparatively easy.

> **NOTE:** According to the Precision Time Protocol (PTP) and Simple Network Time Protocol (SNTP) standards, both protocols can operate in parallel in the same network. However, since both protocols can influence the system time of the device, situations can occur in which the two protocols conflict with each other.

Setting the Time

When there is no reference time source available to you, you can manually set the system time in the device.

When you start the device after it has been powered down for some time, it initializes the clock with January 1 2025, 01:00 UTC+1. After powered down, the device buffers the settings of its real-time clock for up to 24 hours.

As an alternative, you can set up the device to obtain the present time using one of the following protocols:

- Simple Network Time Protocol
- Precision Time Protocol
- 802.1AS protocol

Perform the following steps:

Step	Action
1	Navigate to **Time > Basic Settings** dialog: • The **System time (UTC)** field displays the date and time of the device system clock with reference to Universal Time Coordinated (UTC). UTC is the same worldwide and does not take local time shifts into account. • The time in the **System time** field comes from the System time (UTC) plus the Local offset [min] value and a possible shift due to daylight saving time. **NOTE:** PTP sends the International Atomic Time (TAI). As of July 1, 2020, the TAI time is 37 s ahead of the Universal Time Coordinated (UTC). When the PTP reference time source of the UTC offset is set correctly, the device automatically corrects this difference on the display in the **System time (UTC)** field.
2	To make the device apply the time of your computer to the **System time** field, click **Set time from PC**. Based on the value in the **Local offset [min]** field, the device calculates the time in the **System time (UTC)** field. The System time (UTC) comes from the System time minus the Local offset [min] value and a possible shift due to daylight saving time: • The **Time source** field displays the origin of the time data. The device automatically selects the source with the greatest accuracy. The source is initially **local**. When SNTP is active and the device receives a valid SNTP packet, the device sets its time source to **sntp**. When PTP is active and the device receives a valid PTP message, the device sets its time source to **ptp**. The device prioritizes PTP ahead of SNTP. • The Local offset [min] value specifies the difference in minutes between Universal Time Coordinated (UTC) and local time.
3	To cause the device to determine the time zone on your PC, click **Set time from PC**. The device calculates the difference between local time and Universal Time Coordinated (UTC), and enters the difference into the **Local offset [min]** field. **NOTE:** The device provides the option to obtain the local offset from a DHCP server.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`clock set <YYYY-MM-DD> <HH:MM:SS>`	To set the system time of the device.
`clock timezone offset <-780..840>`	To enter the difference in minutes between the local time and the received Universal Time Coordinated (UTC).
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Automatic Daylight Saving Time Changeover

When you operate the device in a time zone with a summer time change, the device allows automatic daylight saving time changeover.

If the Daylight saving time mode is enabled, the device advances the local system time by one hour during the summer time. At the end of summer time, the device sets the local system time back again by one hour.

Setting Daylight Saving Time Using Pre-Defined Profiles

The device allows the start and end of daylight saving time using pre-defined profiles.

The device includes the following pre-defined profiles:

- EU

  Daylight saving time settings as applicable in the European Union.
- USA

  Daylight saving time settings as applicable in the United States of America.

To select the EU profile for the daylight saving time settings, perform the following steps:

Step	Action
1	Navigate to the **Time > Basic Settings**, **Daylight saving time** tab.
2	In the Operation frame, click **Profile...**.
3	Select the EU item from the Profile... list. Selecting a profile overwrites the settings specified in the Summertime begin and Summertime end frames.
4	Click **OK**.
5	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`clock summer-time mode eu`	To enable the Daylight saving time mode with the profile `eu`.

Setting Daylight Saving Time Manually

The network administrator specifies the following daylight saving time settings:

- Summertime begin:
  - Week = **last**
  - Day = **Sunday**
  - Month = **March**
  - System time = **02:00**
- Summertime end:
  - Week = **last**
  - Day = **Sunday**
  - Month = **October**
  - System time = **03:00**

For the purpose previously described, perform the following steps:

Step	Action
1	Navigate to the **Time > Basic Settings**, **Daylight saving time** tab.
2	Enable the Daylight saving time mode. Select the **On** radio button in the Operation frame.
3	In the Summertime begin frame, specify the following settings: • Week = **last** • Day = **Sunday** • Month = **March** • System time = **02:00**
4	In the Summertime end frame, specify the following settings: • Week = **last** • Day = **Sunday** • Month = **October** • System time = **03:00**
5	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`clock summer-time mode recurring`	To enable the Daylight saving time mode.
`clock summer-time recurring start last sun mar 02:00`	To specify the time at which the device sets the clock forward from standard time to summer time. • `last` To specify the **last** week in the month. • `sun` To specify the day **Sunday**. • `mar` To specify the month **March**. • `02:00` To specify the time **02:00**.
`clock summer-time recurring end last sun oct 03:00`	To specify the time at which the device resets the clock from summer time to standard time. • `last` To specify the **last** week in the month. • `sun` To specify the day **Sunday**. • `oct` To specify the month **October**. • `03:00` To specify the time **03:00**.

Synchronizing Time in the Network with SNTP

The Simple Network Time Protocol (SNTP) allows synchronization of the system time in the network. The device supports the SNTP client and the SNTP server function.

The SNTP server makes the Universal Time Coordinated (UTC) available. UTC is the time relating to the coordinated world time measurement. UTC is the same worldwide and does not take local time shifts into account.

SNTP is a simplified version of Network Time Protocol (NTP). The data packets are identical with SNTP and NTP. Accordingly, both NTP and SNTP servers serve as a time source for SNTP clients.

NOTE: Statements in this chapter relating to external SNTP servers also apply to NTP servers.

SNTP knows the following operation modes for the transmission of time:

- *Unicast*

  In *Unicast* operation mode, an SNTP client sends requests to an SNTP server and expects a response from this server.

- *Broadcast*

  In *Broadcast* operation mode, an SNTP server sends SNTP messages to the network in specified intervals. SNTP clients receive these SNTP messages and evaluate them.

In an IPv6 environment, the *Broadcast* operation mode operates as follows:

- The SNTP client listens only for SNTP server messages that have the IPv6 *multicast* address set to **ff05::101** as the IPv6 destination address.
- The SNTP server sends only SNTP messages to the *multicast* address **ff05::101**. The SNTP server does not send SNTP messages with the link-local address as the IPv6 source address.

The following table presents target IPv4 address classes for Broadcast operation mode:

IPv4 destination address	**Send SNTP packets to**
`0.0.0.0`	Nobody
`224.0.1.1`	*Multicast* address for SNTP messages
`255.255.255.255`	*Broadcast* address

NOTE: An SNTP server in *Broadcast* operation mode also responds to direct requests using *Unicast* from SNTP clients. In contrast, SNTP clients work in either *Unicast* or *Broadcast* operation mode.

Preparation

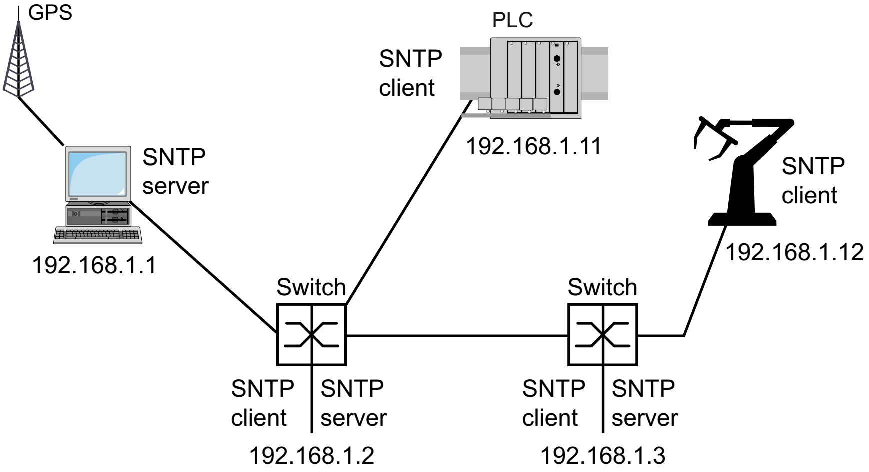
Perform the following steps:

Step 1

To get an overview of how the time is passed on, draw a network plan with the devices participating in SNTP.

When planning, bear in mind that the accuracy of the time depends on the delays of the SNTP messages. To minimize delays and their variance, place an SNTP server in each network segment. Each of these SNTP servers synchronizes its own system time as an SNTP client with its parent SNTP server (SNTP cascade). The highest SNTP server in the SNTP cascade has the most direct access to a reference time source.

The following figure presents an example of the SNTP cascade:



NOTE: For precise time distribution, between SNTP servers and SNTP clients you preferably use network components (routers and switches) that forward the SNTP packets with a low and uniform transmission time (latency).

An SNTP client sends its requests to up to 4 set-up SNTP servers. When there is no response from the first SNTP server, the SNTP client sends its requests to the second SNTP server. When this request is also unsuccessful, it sends the request to the 3rd and finally to the 4th SNTP server. If none of these SNTP servers respond, the SNTP client loses its synchronization. The SNTP client periodically sends requests to each SNTP server until a server delivers a valid time.

NOTE: The device provides the option of obtaining a list of SNTP server IP addresses from a DHCP server.

Step 2

If no reference time source is available to you, determine a device with an SNTP server as a reference time source. Adjust its system time at regular intervals.

Defining Settings of the SNTP Client

As an SNTP client, the device obtains the time information from SNTP or NTP servers and synchronizes its system clock accordingly. To do this, perform the following steps:

Step	Action
1	Navigate to **Time > SNTP > Client**.
2	Set the SNTP operation mode. In the Configuration frame, select one of the following values in the **Mode** field: • **unicast** The device sends requests to an SNTP server and expects a response from this server. • **broadcast** The device waits for *broadcast* or *multicast* messages from SNTP servers on the network.
3	To synchronize the time only once, select the Disable client after successful sync checkbox: • After synchronization, the device disables the Client function. • The table displays the SNTP server to which the SNTP client sends a request in *Unicast* operation mode. The table contains up to 4 SNTP server definitions.
4	To add a table row, click the ⊞ button.
5	Specify the connection data of the SNTP server.
6	Enable the Client function. Select the **On** radio button in the Operation frame.
7	To apply the settings, click the ✓ button. The **State** field displays the present status of the Client function.

The following table presents examples of SNTP client settings:

Device	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Client function	**Off**	**On**	**On**	**On**	**On**
Configuration: Mode	**unicast**	**unicast**	**unicast**	**unicast**	**unicast**
Request interval [s]	**30**	**30**	**30**	**30**	**30**
Server address(es)	**–**	**192.168.1.1**	**192.168.1.2192.168.1.1**	**192.168.1.2192.168.1.1**	**192.168.1.3192.168.1.2192.168.1.1**

Specifying SNTP Server Settings

When operating as an SNTP server, the device distributes its system time as Universal Time Coordinated (UTC) to the network. To do this, perform the following steps:

Step	Action
1	Navigate to **Time > SNTP > Server**.
2	Enable the Server function. Select the **On** radio button in the Operation frame.
3	Enable the *Broadcast* operation mode. Select the **Broadcast admin mode** radio button in the Configuration frame. In *Broadcast* operation mode, the SNTP server sends SNTP messages to the network in specified intervals. The SNTP server also responds to the requests from SNTP clients in *Unicast* operation mode: • In the **Broadcast destination address** field, you set the IPv4 address to which the SNTP server sends the SNTP packets. Set a *broadcast* address or a *multicast* address. In an IPv6 environment, you cannot set the IPv6 address to which the SNTP server sends the SNTP packets. The SNTP server uses the *multicast* address **ff05::101** as the IPv6 destination address. • In the **Broadcast UDP port** field, you specify the number of the UDP port to which the SNTP server sends the SNTP packets in *broadcast* operation mode. • In the **Broadcast VLAN ID** field, you specify the VLAN to which the SNTP server sends the SNTP packets in *broadcast* operation mode. • In the **Broadcast send interval [s]** field, you specify the time interval at which the SNTP server of the device sends SNTP *broadcast* packets. **NOTE:** Except for the **Broadcast destination address** field, the remaining settings are applicable for both IPv4 and IPv6 SNTP servers.
4	To apply the settings, click the ✓ button. The **State** field displays the present status of the Server function.

The following table presents settings for the example:

Device	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.-11	192.168.1.-12
Server function	**On**	**On**	**On**	**Off**	**Off**
UDP port	**123**	**123**	**123**	**123**	**123**
Broadcast admin mode	**cleared**	**cleared**	**cleared**	**cleared**	**cleared**
Broadcast destination address	**0.0.0.0**	**0.0.0.0**	**0.0.0.0**	**0.0.0.0**	**0.0.0.0**
Broadcast UDP port	**123**	**123**	**123**	**123**	**123**
Broadcast VLAN ID	**1**	**1**	**1**	**1**	**1**
Broadcast send interval [s]	**128**	**128**	**128**	**128**	**128**
Disable server at local time source	**cleared**	**cleared**	**cleared**	**cleared**	**cleared**

SynchronizingTime in the Network with PTP

For LAN-controlled applications to operate without latency, precise time management is required. With Precision Time Protocol (PTP), IEEE 1588 describes a method that enables precise synchronization of clocks in the network.

The PTP function in the device permits time synchronization with an accuracy of a few 100 ns. The PTP function uses multicasts for the synchronization messages, therefore keeping the network load low.

Types of Clocks

PTP defines the roles of “master” and “slave” for the clocks in the network:

- A master clock (reference time source) distributes its time.
- A slave clock synchronizes itself with the timing signal received from the master clock.

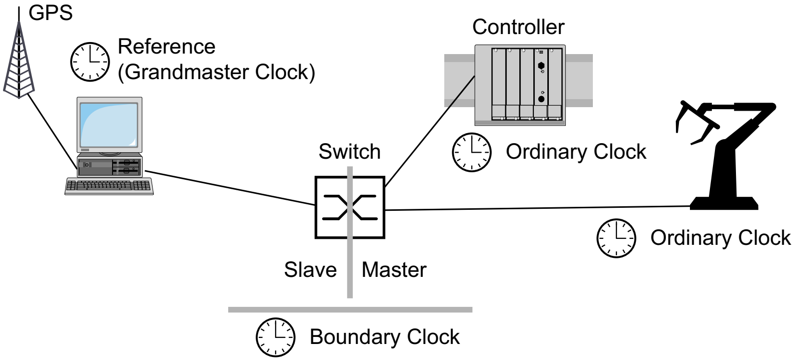
Boundary Clock

The transmission time (latency) in routers and switches has a measurable effect on the precision of the time transmission. To correct such inaccuracies, PTP defines boundary clocks.

In a network segment, a boundary clock is the reference time source (master clock) to which the subordinate slave clocks synchronize. Typically routers and switches take on the role of boundary clock.

The boundary clock in turn obtains the time from a greater-level reference time source (Grandmaster).

The following figure illustrates the position of the boundary clock in a network:



Transparent Clock

Switches typically take on the *Transparent Clock* role to enable high accuracy across the cascades. The *Transparent Clock* is a *Slave* clock that corrects its own transmission time when it forwards received synchronization messages.

Ordinary Clock

PTP designates the clock in an end device as an *Ordinary Clock*. An *Ordinary Clock* functions either as a master clock or slave clock.

Best Master Clock Algorithm

The devices participating in PTP designate a device in the network as a reference time source (Grandmaster). Here the *Best Master Clock* algorithm is used, which determines the accuracy of the clocks available in the network.

The *Best Master Clock* algorithm evaluates the following criteria:

- Priority 1

- Clock class
- Clock accuracy
- Clock variance
- Priority 2

The algorithm first evaluates the value in the **Priority 1** field of the participating devices. The device with the numerically lowest value in the **Priority 1** field is designated as the reference time source (*Grandmaster*). If the value is the same for multiple devices, the algorithm takes the next criterion. If this is also the same, the algorithm takes the next criterion after this one. If these values are the same for multiple devices, the numerically lowest value in the **Clock identity** field determines which device is designated as the reference time source (*Grandmaster*). The value in the **Clock identity** field is based on the device MAC address which is supposed to be globally unique. The value in the **Clock identity** field serves as the final tie-break for the algorithm.

In the settings of the boundary clock, the device allows values to be specified for Priority 1 and Priority 2. This allows influence on which device will be the reference time source (*Grandmaster*) in the network.

Delay Measurement

The delay of the synchronization messages between the devices affects the accuracy. The delay measurement allows devices to take into account the average delay.

PTP version 2 offers the following methods for delay measurement:

- **e2e** (End to End)

  The slave clock measures the delay of synchronization messages to the master clock.
- **e2e-optimized**

  The slave clock measures the delay of synchronization messages to the master clock.

  This method is available only for transparent clocks. The device forwards the synchronization messages sent using multicast only to the master clock, keeping the network load low. When the device receives a synchronization message from another master clock, it forwards the synchronization messages only to this new port.

  When the device does not have a master clock defined, it forwards synchronization messages to every port.
- **p2p** (Peer to Peer)

  The slave clock measures the delay of synchronization messages to the master clock.

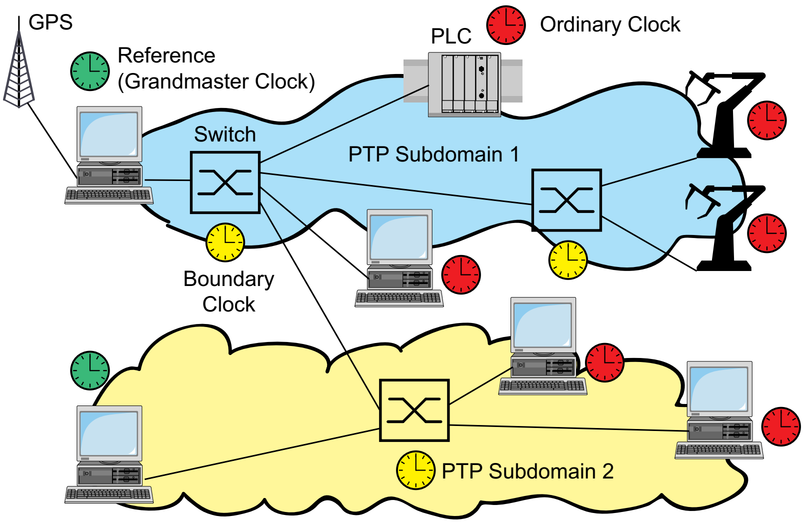
  In addition, the master clock measures the delay to each slave clock, even across blocked ports. This requires that the master and slave clocks support Peer-to-Peer (**p2p**).

  In case of interruption of a redundant ring, for example, the slave clock becomes the master clock and the master clock becomes the slave clock. This switch occurs without loss of precision, because the clocks already account for the delay in the other direction.

PTP Domains

The device transmits synchronization messages only from and to devices in the same PTP domain. The device allows the domain to be set for the boundary clock and the transparent clock individually.

The following figure presents an example of PTP domains:



Using PTP

To synchronize the clocks precisely with PTP, only use switches with a boundary clock or transparent clock as nodes.

Perform the following steps:

- To gain an overview of the distribution of clocks, draw a network plan with the devices involved in PTP.
- Specify the role for each participating switch (boundary clock or transparent clock). In the device, this setting is called PTP mode.

  The following table presents possible settings for PTP mode:

PTP mode	Application
v2-boundary-clock	As a boundary clock, the device distributes synchronization messages to the slave clocks in the subordinate network segment. The boundary clock in turn obtains the time from a greater-level reference time source (Grandmaster).
v2-transparent-clock	As a transparent clock, the device forwards received synchronization messages after they have been corrected by the delay of the transparent clock.

- Enable PTP on each participating switch.

  PTP then sets itself up on a largely automatic basis.
- Enable PTP on the end devices.
- The device allows influence on which device in the network becomes the (Grandmaster). Therefore, change the default value in the **Priority 1** and **Priority 2** fields for the *Boundary Clock*.

Synchronizing Time in the Network with 802.1AS

Some LAN-based applications require the internal clocks of the participating devices to be precisely synchronized. The IEEE 802.1AS-2020 protocol describes a method that enables precise synchronization of the clocks of time-aware devices in the network.

The IEEE 802.1AS-2020 protocol is based on Precision Time Protocol (PTP) and is tailored for Ethernet-based Time-Sensitive Networking (TSN) environments.

The 802.1AS function in the device permits time synchronization with an accuracy of a few 100 ns. The 802.1AS function uses multicast for the synchronization messages, therefore keeping the network load low.

Instances and Domains

Each *PTP domain* operates independently and helps ensure that the clocks of the time-aware devices within the *PTP domain* are synchronized. The devices are synchronized to the reference time source (*Grandmaster*) of the respective domain. You can use different domains to synchronize the time for different groups of devices within a network.

The device can be part of multiple *PTP domains*. In the device, the 802.1AS function supports 2 instances: *Instance 0* and *Instance 1*, each operating within separate *PTP domains*.

You set up each instance separately:

- *Instance 0*

  for synchronizing device clocks and transmitting time synchronization messages
- *Instance 1*

  only for transmitting time synchronization messages

Best Master Clock Algorithm

The devices participating in PTP designate a device in the *PTP domain* as a reference time source (*Grandmaster*). The *Best Master Clock* algorithm is used to determine the accuracy of the clocks available in the *PTP domain*.

The *Best Master Clock* algorithm evaluates the following criteria for each participating device:

- Priority 1
- Clock class
- Clock accuracy
- Clock variance
- Priority 2
- Clock identity

The algorithm first evaluates the value in the **Priority 1** field of the participating devices. The device with the numerically lowest value in the **Priority 1** field is designated as the reference time source (*Grandmaster*). If the value is the same for multiple devices, the algorithm takes the next criterion. If this is also the same, the algorithm takes the next criterion after this one. If these values are the same for multiple devices, the numerically lowest value in the **Clock identity** field determines which device is designated as the reference time source (*Grandmaster*). The value in the **Clock identity** field is based on the device MAC address which is supposed to be globally unique. The value in the **Clock identity** field serves as the final tie-break for the algorithm.

Enabling the 802.1AS Function

The 802.1AS function and the PTP function cannot be enabled simultaneously on the device.

In the default setting, the 802.1AS function is disabled. Enabling the 802.1AS function allows time-aware devices within the same *PTP domain* to synchronize.

Perform the following steps on each device within the same *PTP domain*:

Step	Action
1	Navigate to **Time > 802.1AS > Global**.
2	Enable the 802.1AS function globally. Select the **On** radio button in the Operation frame.
3	To apply the settings, click the ✓ button.
4	Navigate to **Time > 802.1AS > Port**.
5	Enable the 802.1AS function for *Instance 0/* • Select the *Instance 0* tab. • Select the **On** radio button in the Operation frame.
6	Enable the 802.1AS function on the interface. In the Active column of the desired interface, select the checkbox.
7	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dot1as operation enable`	To enable the 802.1AS function globally.
`dot1as instance 0 operation enable`	To enable the 802.1AS function for *Instance 0*.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`dot1as instance 0 operation enable`	To enable the 802.1AS function on interface **1/1** for *Instance 0*.
`show dot1as data-port-set instance 0 port 1/1`	To verify the status of *Instance 0* on interface **1/1**.
`show dot1as current instance 0`	To verify the status of *Instance 0*.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, refer to Saving a Configuration Profile, page 87.

Disabling the 802.1AS Function Globally

When disabling the 802.1AS function globally, you disable time synchronization for both instances and for the respective ports allocated to them. This disables time synchronization on the instance and port levels even if the 802.1AS function is enabled on the instances and on the individual ports.

Perform the following steps on each device within the same *PTP domain*:

Step	Action
1	Navigate to **Time > 802.1AS > Global**.
2	Disable the 802.1AS function globally: • Select the **Off** radio button in the Operation frame.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dot1as operation disable`	To disable the 802.1AS function globally.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, refer to Saving a Configuration Profile, page 87.

Disabling the 802.1AS Function for an Instance

You disable the 802.1AS function on an instance, for example, in the following situations:

- To disable time synchronization for the ports allocated to the respective instance in a single action
- To reallocate a port from one instance to another instance
- To reduce the network load generated by the transmission of synchronization messages

Perform the following steps:

Step	Action
1	Navigate to **Time** > **802.1AS** > **Port**.
2	Disable the 802.1AS function for *Instance 0*: • Select the *Instance 0* tab. Select the **Off** radio button in the Operation frame.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dot1as instance 0 operation disable`	To disable the 802.1AS function for *Instance 0*.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, refer to Saving a Configuration Profile, page 87.

Disabling the 802.1AS Function on a Port

You disable the 802.1AS function on an individual port, for example, in the following situations:

- When the port is connected to a device that is not time-aware and, therefore, does not require time synchronization.
- When you allocate the port to another instance. Before you allocate a port to another instance, disable the 802.1AS function on the port.

Perform the following steps:

Step	Action
1	Navigate to **Time > 802.1AS > Port** dialog: • Select the *Instance 0* tab.
2	Deactivate the 802.1AS function on interface **1/1**: • Clear the checkbox in the Active column.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`dot1as instance 0 operation disable`	To disable the 802.1AS function on interface **1/1** for *Instance 0*.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, refer to Saving a Configuration Profile, page 87.

Managing Configuration Profiles

If you change the settings of the device during operation, the device stores the changes in its memory (RAM). After a reboot the settings are lost.

To keep the changes after a reboot, the device allows the settings to be saved in a configuration profile in the non-volatile memory (**NVM**). To make it possible to switch to other settings, the non-volatile memory (**NVM**) offers storage space for multiple configuration profiles.

If an external memory is connected, the device automatically registers a copy of the configuration profile in the external memory. You can disable this function.

Detecting Changed Settings

The device stores changes made to settings during operation in its volatile memory (**RAM**). The configuration profile in the non-volatile memory (**NVM**) remains unchanged until you save the changed settings explicitly. Until then, the configuration profiles in memory and non-volatile memory (**NVM**) are different. The device helps you recognize changed settings.

Volatile Memory (RAM) and Non-Volatile Memory (NVM)

You can recognize if the settings in the volatile memory (**RAM**) differ from the settings of the **Selected** configuration profile in the non-volatile memory (**NVM**). To do this, perform the following steps:

Step	Action
1	Verify the banner of the Graphical User Interface: • When the flashing icon 💾! is visible, the settings differ. • When no flashing icon 💾! is visible, the settings match.

Or:

Step	Action
1	Navigate to **Basic Settings > Load/Save**.
2	Verify the status of the checkbox in the Information frame: • When the checkbox is selected, the settings match. • When the checkbox is cleared, the settings differ.

The following commands are available:

```
show config status

Configuration Storage sync State
--------------------------------
running-config to NV........................out of sync
...
```

External Memory (ENVM) and Non-Volatile Memory (NVM)

You can recognize if the settings copied to the external memory (**ENVM**) differ from the settings of the configuration profile in the non-volatile memory (**NVM**). To do this, perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Load/Save**.
2	Verify the status of the checkbox in the Information frame: • When the checkbox is selected, the settings match. • When the checkbox is cleared, the settings differ.

The following commands are available:

```
show config status

Configuration Storage sync State
--------------------------------
...
NV to EAM...................................out of sync
...
```

Saving the Settings

Saving the Configuration Profile in the Switch

If you change the settings of the device during operation, the device stores the changes in its memory (**RAM**). To keep the changes after a reboot, save the configuration profile in the non-volatile memory (**NVM**).

Saving a Configuration Profile

The device stores the settings in the **Selected** configuration profile in the non-volatile memory (**NVM**).

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Load/Save**.
2	Verify that the required configuration profile is **Selected**. You can recognize a **Selected** configuration profile with the checkbox in the **Selected** column.
3	Click the 💾 button.

Execute the following commands:

Command	Description
`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (**nvm**).
`enable`	To change to the Privileged EXEC mode.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Copying Settings to a Configuration Profile

The device allows settings saved in the memory (**RAM**) to be stored in a configuration profile other than the **Selected** configuration profile. In this way the device adds a configuration profile in the non-volatile memory (**NVM**) or overwrites an existing one.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Load/Save**.
2	Click the ☰ button, then select **Save as...**. The dialog displays the Save as... window.
3	In the **Name** field, change the name of the configuration profile. If you keep the proposed name, the device will overwrite an existing configuration profile of the same name.
4	Click **OK**. The new configuration profile is designated as **Selected**.

Execute the following commands:

Command	Description
`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (**nvm**).
`enable`	To change to the Privileged EXEC mode.
`copy config running-config nvm profile <string>`	To save the updated settings in the configuration profile named **<string>** in the non-volatile memory (**nvm**). If present, the device overwrites a configuration profile of the same name. The new configuration profile is designated as **Selected**.

Selecting a Configuration Profile

When the non-volatile memory (**NVM**) contains multiple configuration profiles, you have the option to select any configuration profile there. The device stores the settings in the **Selected** configuration profile. During the system startup, the device loads the settings of the **Selected** configuration profile into the memory (**RAM**).

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Load/Save**. The table displays the configuration profiles present in the device. You can recognize the **Selected** configuration profile with the checkbox in the **Selected** column.
2	Select the table row of the desired configuration profile stored in the non-volatile memory (**NVM**).
3	Click the ☰ button, then click **Select**. In the **Selected** column, the checkbox of the configuration profile is now selected.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (**nvm**).
`configure`	To change to the Configuration mode.
`config profile select nvm 1`	To select the configuration profile. Take note of the adjacent name of the configuration profile.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Saving the Configuration Profile in the External Memory (ENVM)

When an external memory (**ENVM**) is connected and you save a configuration profile, the device automatically saves a copy in the selected external memory. In the default setting, the function is enabled. You can disable this function.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > External Memory**.
2	Select the checkbox in the Backup config when saving column to enable the device to automatically save a copy in the external memory (**ENVM**) during the saving process.
3	To deactivate the function, clear the checkbox in the Backup config when saving column.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`config envm config-save usb`	To enable the function. When you save a configuration profile, the device saves a copy in the external memory (**ENVM**). **usb** = External USB memory
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Backing Up the Configuration Profile on a Remote Server

The device allows automatic backup of the configuration profile to a remote server. The prerequisite is that you activate the function before you save the configuration profile.

After you save the configuration profile in the non-volatile memory (**NVM**), the device sends a copy to the specified URL.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Load/Save**.
2	In the **Backup config on a remote server when saving** frame, perform the following steps: • In the URL field, specify the server as well as the path and file name of the backed up configuration profile. • Click **Set credentials**. The dialog displays the Credentials window.
3	Enter the login credentials needed to authenticate on the remote server.
4	In the Operation option list, enable the function.
5	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`show config remote-backup`	To verify the status of the function.
`configure`	To change to the Configuration mode.
`config remote-backup destination {URL}`	To enter the destination URL for the configuration profile backup (max. 128 chars).
`config remote-backup username {username}`	To enter the user name to authenticate on the remote server (max. 128 chars).
`config remote-backup password {password}`	To enter the password to authenticate on the remote server (max. 128 chars).
`config remote-backup operation`	To enable the function.

If the transfer to the remote server is unsuccessful, the device logs this event in the System Log.

Exporting a Configuration Profile

The device allows a configuration profile to be saved to a server as an XML file. If you use the Graphical User Interface, you have the option to save the XML file directly to your PC.

Prerequisites:

- To save the file on a server, you need a server available on the network.
- To save the file to an SCP or SFTP server, you also need the user name and password for accessing this server.
- Ensure the SCP or SFTP server is defined by the device before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Load/Save**.
2	Select the table row of the desired configuration profile.

Export the configuration profile to your PC. To do this, perform the following step:

- Click the link in the **Profile name** column.

  The configuration profile is downloaded and saved as an XML file on your PC.

Export the configuration profile to a remote server. To do this, perform the following steps:

Step	Action
1	Click the ≡ button, then select **Export**. The dialog displays the Export... window.
2	In the URL field, specify the file URL on the remote server: • To save the file on an FTP server, specify the URL for the file in the following form: ftp://<user>:<password>@<IP address>[:port]/<file name> Do not use this method if you transmit data over untrusted networks. • To save the file on a TFTP server, specify the URL for the file in the following form: tftp://<IP address>/<path>/<file name> Do not use this method if you transmit data over untrusted networks. • To save the file on an SCP or SFTP server, specify the URL for the file in one of the following forms: scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name> scp:// or sftp://<IP address>/<path>/<file name> Ensure the SCP or SFTP server is defined by the device before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog. When you click **OK**, the device displays the Credentials window. There you enter User name and Password to log into the server.
3	Click **OK**. The configuration profile is now saved as an XML file in the specified location.

Execute the following commands:

Command	Description
`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (**nvm**).
`enable`	To change to the Privileged EXEC mode.
`copy config running-config remote tftp://<IP_address>/<path>/<file_name>`	To save the updated settings on a TFTP server. Do not use this method if you transmit data over untrusted networks.
`copy config nvm remote  sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>`	To save the **Selected** configuration profile in the non-volatile memory (**nvm**) on a SFTP server.
`copy config nvm  profile config3  remote tftp://<IP_address>/   <path>/<file_name>`	To save the configuration profile **config3** in the non-volatile memory (**nvm**) on a TFTP server. Do not use this method if you transmit data over untrusted networks.
`copy config nvm  profile config3  remote ftp://<IP_address>[:port]/<path>/<file_name>`	To save the configuration profile **config3** in the non-volatile memory (**nvm**) on an FTP server. Do not use this method if you transmit data over untrusted networks.

Loading Settings

If you save multiple configuration profiles in the memory, you have the option to load a different configuration profile.

Activating a Configuration Profile

The non-volatile memory of the device can contain multiple configuration profiles. If you activate a configuration profile stored in the non-volatile memory (**NVM**), you must immediately change the settings in the device. The device does not require a reboot.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Load/Save**.
2	Select the table row of the desired configuration profile.
3	Click the ☰ button, then select **Activate**. The device copies the settings to the memory (**RAM**) and disconnects from the Graphical User Interface. The device immediately uses the settings of the configuration profile.
4	Reload the Graphical User Interface.
5	Log in again. In the **Selected** column, the checkbox of the configuration profile that was activated before is selected.

Execute the following commands:

Command	Description
`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (**nvm**).
`enable`	To change to the Privileged EXEC mode.
`copy config nvm profile config3 running-config`	To activate the settings of the configuration profile **config3** in the non-volatile memory (**nvm**). The device copies the settings into the volatile memory and disconnects the connection to the Command Line Interface. The device immediately uses the settings of the configuration profile **config3**.

Loading the Configuration Profile from the External Memory (ENVM)

If an external memory (**ENVM**) is connected, the device loads a configuration profile from the external memory during the system startup automatically. The device allows these settings to be saved in a configuration profile in non-volatile memory (**NVM**).

When the external memory contains the configuration profile of an identical device, you have the possibility to transfer the settings from one device to another.

Perform the following step:

- Verify that the device loads a configuration profile from the external memory during the system startup.

In the default setting, the function is enabled. If the function is disabled, enable it again as follows:

Step	Action
1	Navigate to **Basic Settings > External Memory**.
2	In the Config priority column, select the value **first**.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`config envm load-priority usb first`	To enable the function. During the system startup, the device loads a configuration profile from the external memory (**ENVM**). **usb** = External USB memory
`show config envm settings`	To display the settings of the external memory (**ENVM**).

`Type   Status      Auto Update Save Config Config Load Prio`
`------ ----------- ----------- ----------- ----------------`	

`usb    ok          [x]         [x]         first`	
`save`	To save the settings in a configuration profile in the non-volatile memory (**NVM**) of the device.

Using the Command Line Interface, the device allows the settings from the external memory (**ENVM**) to be copied directly to the non-volatile memory (**NVM**).

Execute the following commands:

Command	Description
`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (**nvm**).
`enable`	To change to the Privileged EXEC mode.
`copy config envm profile config3 nvm`	To copy the configuration profile **config3** from the external memory (**ENVM**) to the non-volatile memory (**NVM**).

The device can also automatically load a configuration profile from a script file during the system startup.

Prerequisites:

- Verify that the external memory (**ENVM**) is connected before you start the device.
- The root directory of the external memory (**ENVM**) contains a text file startup. txt with the content `script=<file_name>`. The placeholder `<file_name>` represents the script file that the device executes during the system startup.
- The root directory of the external memory (**ENVM**) contains the script file. You have the option to save the script with a user-specified name. Save the file with the file extension .cli.

  NOTE: Verify that the script saved in the external memory (**ENVM**) is not empty. If the script is empty, the device loads the next configuration profile as per the configuration priority settings.

After applying the script, the device automatically saves the configuration profile from the script file as an XML file in the external memory (**ENVM**).

When you type the appropriate command into the script file, you have the option to disable this function with the following command:
`no config envm config-save usb`
The device does not save a copy in the external USB memory.

When the script file contains an incorrect command, the device does not apply this command during the system startup. The device logs the event in the System Log.

Importing a Configuration Profile

The device allows a configuration profile saved as an XML file to be imported from a server. If you use the Graphical User Interface, you can import the XML file directly from your PC.

Prerequisites:

- To import a file from a server, you need a server available on the network.
- To import a file from an SCP or SFTP server, you also need the user name and password for accessing this server.
- Ensure that the SCP or SFTP server is defined to the device before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings** > **Load/Save**.
2	Click the ☰ button, then select **Import**. The dialog displays the Import... window.
3	From the Select source drop-down list, select the location from where the device imports the configuration profile: • **PC/URL** The device imports the configuration profile from the local PC or from a remote server. • **External memory** The device imports the configuration profile from the external memory (**ENVM**).

Import the configuration profile from the local PC or from a remote server. To do this, perform the following steps:

Step	Action
1	Import the configuration profile: • When the file is located on your PC or on a network drive, drag and drop it onto the ⭱ area. As an alternative, click in the area to select the file. • If the file is on an FTP server, specify the URL in the following form: ftp://<user>:<password>@<IP address>[:port]/<file name> Do not use this method if you transmit data over untrusted networks. • If the file is on a TFTP server, specify the URL in the following form: tftp://<IP address>/<path>/<file name> Do not use this method if you transmit data over untrusted networks. • If the file is on an SCP or SFTP server, specify the URL in one of the following forms: scp:// or sftp://<IP address>/<path>/<file name> When you click **Start**, the device displays the Credentials window. There you enter User name and Password to log into the server. scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name> Ensure that the SCP or SFTP server is defined by the device before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog.
2	In the Destination frame, specify where the device saves the imported configuration profile: • In the **Profile name** field, specify the name under which the device saves the configuration profile. • In the **Storage** field, specify the storage location for the configuration profile.
3	Click **OK**. The device copies the configuration profile into the specified memory. If you specified the value **ram** in the Destination frame, the device disconnects the Graphical User Interface and uses the settings immediately.

Import the configuration profile from the external memory (**ENVM**). To do this, perform the following steps:

Step	Action
1	In the Import profile from external memory frame, select the name of the configuration profile to be imported from the Profile name drop-down list. The prerequisite is that the external memory (**ENVM**) contains an exported configuration profile.
2	In the Destination frame, specify where the device saves the imported configuration profile: • In the **Profile name** field, specify the name under which the device saves the configuration profile.
3	Click **OK**. The device copies the configuration profile into the non-volatile memory (**NVM**) of the device. If you specified the value **ram** in the Destination frame, the device disconnects the Graphical User Interface and uses the settings immediately.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`copy config remote ftp://<IP_address>[:port]/<path>/<file_name> running-config`	To import and activate the settings of a configuration profile saved on an FTP server. Do not use this method if you transmit data over untrusted networks. The device copies the settings into the volatile memory and disconnects the connection to the Command Line Interface. The device immediately uses the settings of the imported configuration profile.
`copy config  remote tftp://<IP_address>/   <path>/<file_name>  running-config`	To import and activate the settings of a configuration profile saved on a TFTP server. Do not use this method if you transmit data over untrusted networks. The device copies the settings into the volatile memory and disconnects the connection to the Command Line Interface. The device immediately uses the settings of the imported configuration profile.
`copy config remote  sftp://<user name>:<password>@<IP_address>/<path>/<file_name> running-config`	To import and activate the settings of a configuration profile saved on a SFTP server. The device copies the settings into the volatile memory and disconnects the connection to the Command Line Interface. The device immediately uses the settings of the imported configuration profile.
`copy config  remote ftp://<IP_address>[:port]/<path>/<file_name>    nvm profile config3`	To import the settings of a configuration profile saved on an FTP server and save the settings in the configuration profile **config3** in the non-volatile memory (**nvm**). Do not use this method if you transmit data over untrusted networks.
`copy config  remote tftp://<IP_address>/<path>/<file_name> nvm profile config3`	To import the settings of a configuration profile saved on a TFTP server and save the settings in the configuration profile **config3** in the non-volatile memory (**nvm**). Do not use this method if you transmit data over untrusted networks.

Resetting the Switch to the Default Setting

If you reset the settings in the device to the delivery state, the device deletes the configuration profiles in the volatile memory and in the non-volatile memory.

If an external memory (**ENVM**) is connected, the device also deletes the configuration profiles saved in the external memory (**ENVM**).

The device then reboots and loads the factory settings.

Using the Graphical User Interface or Command Line Interface

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Load/Save**.
2	Click the ☰ button, then select **Back to factory...**. The dialog displays a message.
3	Click **OK**. The device deletes the configuration profiles in the memory (**RAM**) and in the non-volatile memory (**NVM**). If an external memory (**ENVM**) is connected, the device also deletes the configuration profiles saved in the external memory (**ENVM**). After a brief period, the device restarts and loads the delivery settings.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`clear factory`	To delete the configuration profiles from the non-volatile memory (**NVM**) and from the external memory (**ENVM**). If an external memory (**ENVM**) is connected, the device also deletes the configuration profiles saved in the external memory (**ENVM**). After a brief period, the device restarts and loads the delivery settings.

Using System Monitor 1

Perform the following steps:

- To change to System Monitor 1, proceed as described in Access to Switch Management, page 33.
- To change from the main menu to the `Manage configurations` menu, press the **4** key.
- To execute the `Clear configs and boot params` command, press the **1** key.
- To load the factory settings, press the **Enter** key.

  The device deletes the configuration profiles in the memory (**RAM**) and in the non-volatile memory (**NVM**).

  If an external memory (**ENVM**) is connected, the device also deletes the configuration profiles saved in the external memory (**ENVM**).
- To change to the main menu, press the **q** key.
- To reboot the device with factory settings, press the **q** key.

Updating the Switch Software

Schneider Electric is continually working on improving and developing their software. Verify regularly if there is an updated version of the device software on the Schneider Electric product pages on the Internet at https://www.se.com/ww/en/download/.

The device gives you the following options to update the device software:

- Loading a Previous Switch Software Version, page 98
- Software Update from the PC, page 98
- Software Update from a Server, page 99
- Software Update from the External Memory (ENVM), page 104

NOTE: The device settings are kept after you update the device software.

You can see the version of the installed device software in the login dialog of the Graphical User Interface.

To display the version of the installed device software when you are already logged into the device management, perform the following step:

- Navigate to **Basic Settings > Software**.

  The **Running version** field displays the version number and creation date of the running device software that the device loaded during the last system startup.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`show system info`	To display the system information such as the version number and creation date of the running device software that the device loaded during the last system startup.

Loading a Previous Switch Software Version

The device allows replacement of the device software with a previous version. The basic settings in the device are kept after replacing the device software.

If the Secure Boot function is active, you cannot downgrade to a software version earlier than 10.0.00. See the **Basic Settings > Software** dialog, Software update frame.

NOTE: Only the settings for functions which are available in the newer device software version are lost.

Software Update from the PC

The device allows update of the device software, if a suitable device software image is saved on a storage medium which is accessible from your PC.

To remain logged in to the device management during the software update, move the mouse pointer occasionally. As an alternative, before you start the software update, specify a sufficiently high value in the **Device Security > Management Access > Web** dialog, **Web interface session timeout [min]** field.

Perform the following steps:

Step	Action
1	Navigate to the folder where the device software image is saved.
2	Navigate to **Basic Settings** > **Software**.
3	Drag and drop the file into the ⬆ area. As an alternative, click in the area to select the file.
4	Start the software update. To do this, click **Start**. • The device transfers the previously used device software to the backup memory. • The device transfers the selected file to the flash memory, replacing the previously used device software. As soon as the update procedure is completed successfully, the device displays a success notification. During the next startup, the device boots with the device software that you have transferred.

Software Update from a Server

The device allows update of its software if you have access to a server where a suitable device software image is saved.

The device gives you the following options to update the device software:

- Software Update from an FTP Server, page 99
- Software Update from a TFTP server, page 100
- Software Update from an SFTP Server, page 101
- Software Update from an SCP Server, page 102

To remain logged in to the device management during the software update, move the mouse pointer occasionally. As an alternative, before you start the software update, specify a sufficiently high value in the **Device Security > Management Access > Web** dialog, **Web interface session timeout [min]** field.

Software Update from an FTP Server

This option allows update of the device software image from an FTP server.

Do not use this method if you transmit data over untrusted networks.

The prerequisite is that the access role **administrator** is assigned to the user account you use to perform the actions on the device.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Software**.
2	In the **Software update frame, URL** field, specify the URL for the device software image using the following format: ftp://user:password@IP_address:port/path/to/software_image.bin You can also specify the URL without the user name and password. In this case, enter them in the Credentials window after clicking **Start**.
3	Click **Start**. • The device transfers the previously used device software to the backup memory. • The device transfers the selected file to the flash memory, replacing the previously used device software. As soon as the update procedure is completed successfully, the device displays an information that the device software was successfully updated. During the next startup, the device boots with the device software that you have transferred.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`copy firmware remote ftp://user:password@10.0.1.159:21/path/to/software_image.bin system`	To transfer the device software image from an FTP server to the flash memory of the device. • `copy firmware remote` To copy the device software image from a remote location. • `ftp://user:password@10.0.1.159:21/path/to/software_image.bin` URL of the FTP server where the device software image file is saved. You can also specify the URL without the user name and password. In this case, the device will prompt you to enter the missing information afterwards. ◦ `ftp://` Protocol for the file transfer ◦ `user` User account name of the FTP server ◦ `password` User account password ◦ `10.0.1.159` IP address of the FTP server ◦ `21` Default port for FTP ◦ `/path/to/` The path to the device software image on the FTP server ◦ `software_image.bin` Name of the device software image • `system` To transfer the copied device software image to the flash memory.

Software Update from a TFTP Server

This option allows update of the device software image from a TFTP server.

Do not use this method if you transmit data over untrusted networks.

The prerequisite is that the access role **administrator** is assigned to the user account you use to perform the actions on the device.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Software**.
2	In the **Software update frame, URL** field, specify the URL for the device software image using the following format: tftp://IP_address/path/to/software_image.bin
3	Click **Start**. • The device transfers the previously used device software to the backup memory. • The device transfers the selected file to the flash memory, replacing the previously used device software. As soon as the update procedure is completed successfully, the device displays an information that the device software was successfully updated. During the next startup, the device boots with the device software that you have transferred.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`copy firmware remote tftp://10.0.1.159/path/to/software_image.bin system`	To transfer the device software image from a TFTP server to the flash memory of the device. • `copy firmware remote` To copy the device software image from a remote location. • `tftp://10.0.1.159/path/to/software_image.bin` URL of the TFTP server where the device software image is saved. ◦ `tftp://` Protocol for the file transfer ◦ `10.0.1.159` IP address of the TFTP server ◦ `/path/to/` The path to the device software image on the TFTP server ◦ `software_image.bin` Name of the device software image • `system` To transfer the copied device software image to the flash memory.

Software Update from an SFTP Server

This option allows update of the device software image from an SFTP server.

Prerequisites:

- The access role **administrator** is assigned to the user account you use to perform the actions on the device.
- The SFTP server is defined by the device. See the **Device Security > SSH Known Hosts** dialog.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Software**.
2	In the **Software update frame, URL** field, specify the URL for the device software image using the following format: sftp://user:password@IP_address/path/to/software_image.bin You can also specify the URL without the user name and password. In this case, enter them in the Credentials window after clicking **Start**.
3	Click **Start**. • The device transfers the previously used device software to the backup memory. • The device transfers the selected file to the flash memory, replacing the previously used device software. As soon as the update procedure is completed successfully, the device displays an information that the device software was successfully updated. During the next startup, the device boots with the device software that you have transferred.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`copy firmware remote sftp://user:password@10.0.1.159:21/path/to/software_image.bin system`	To transfer the device software image from an SFTP server to the flash memory of the device. • `copy firmware remote` To copy the device software image from a remote location. • `sftp://user:password@10.0.1.159:21/path/to/software_image.bin` URL of the SFTP server where the device software image is saved. You can also specify the URL without the user name and password. In this case, the device will prompt you to enter the missing information afterwards. ◦ `sftp://` Protocol for the file transfer ◦ `user` User account name of the SFTP server ◦ `password` User account password ◦ `10.0.1.159` IP address of the SFTP server ◦ `/path/to/` The path to the device software image on the SFTP server ◦ `software_image.bin` Name of the device software image • `system` To transfer the copied device software image to the flash memory.

Software Update from an SCP Server

This option allows update of the device software image from an SCP server.

Prerequisites:

- The access role **administrator** is assigned to the user account you use to perform the actions on the device.
- The SCP server is defined by the device. See the **Device Security > SSH Known Hosts** dialog.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Software**.
2	In the **Software update frame, URL** field, specify the URL for the device software image using the following format: scp://user:password@IP_address/path/to/software_image.bin You can also specify the URL without the user name and password. In this case, enter them in the Credentials window after clicking **Start**.
3	Click **Start**. • The device transfers the previously used device software to the backup memory. • The device transfers the selected file to the flash memory, replacing the previously used device software. As soon as the update procedure is completed successfully, the device displays an information that the device software was successfully updated. During the next startup, the device boots with the device software that you have transferred.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`copy firmware remote scp://user:password@10.0.1.159:21/path/to/software_image.bin system`	To transfer the device software image from an SCP server to the flash memory of the device. • `copy firmware remote` To copy the device software image from a remote location. • `user:password@10.0.1.159:21/path/to/software_image.bin` URL of the SCP server where the device software image is saved. You can also specify the URL without the user name and password. In this case, the device will prompt you to enter the missing information afterwards. ◦ `scp://` Protocol for the file transfer ◦ `user` User account name of the SCP server ◦ `password` User account password ◦ `10.0.1.159` IP address of the SCP server ◦ `/path/to/` The path to the device software image on the SCP server ◦ `software_image.bin` Name of the device software image • `system` To transfer the copied device software image to the flash memory.

Software Update from the External Memory (ENVM)

Manually-Initiated by the Administrator

The device allows update of the software. The prerequisite is that the image file of the software is located in the external memory.

To remain logged in to the device management during the software update, move the mouse pointer occasionally. As an alternative, before you start the software update, specify a sufficiently high value in the **Device Security > Management Access > Web** dialog, **Web interface session timeout [min]** field.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Load/Save**.
2	In the External memory frame, verify that the relevant external memory is selected from the **Selected external memory** drop-down list.
3	Navigate to **Basic Settings > Software**.
4	Select the table row for which the File location column displays the value **usb**.
5	Start the software update. To do this, click the ⬆ button. • The device transfers the previously used device software to the backup memory. • The device transfers the selected file to the flash memory, replacing the previously used device software. As soon as the update procedure is completed successfully, the device displays a success notification. During the next startup, the device boots with the device software that you have transferred.

Automatically-Initiated by the Switch

When the following files are located in the external memory (**ENVM**) during the system startup, the device updates the device software automatically:

- The device software image
- A text file startup.txt with the content `autoUpdate=<software_image_file_name>.bin`

The prerequisite is that in the **Basic Settings > External Memory** dialog, you select the checkbox in the Software auto update column. This is the default setting in the device.

Perform the following steps:

Step	Action
1	Transfer the new device software image into the main directory of the external memory (**ENVM**). Use only a device software image suitable for the device.
2	Create a text file startup.txt in the main directory of the external memory (**ENVM**).
3	Open the startup.txt file in the text editor and add the following line: `autoUpdate=<software_image_file_name>.bin`
4	Install the external memory (**ENVM**) in the device.
5	Restart the device. During the booting process, the device verifies automatically the following criteria: • Is an external memory (**ENVM**) connected? • Is a startup.txt file in the main directory of the external memory (**ENVM**)? • Does the device software image exist which is specified in the startup. txt file? • Does the software have a newer version than the version the device is using?
6	When the criteria are fulfilled, the device starts the update procedure. The device copies the running device software into the backup memory. As soon as the update procedure is completed successfully, the device reboots automatically and loads the new device software version.
7	Verify the result of the update procedure. The log file in the **Diagnostics > Report > System Log** dialog contains one of the following messages: • **S_watson_AUTOMATIC_SWUPDATE_SUCCESS** Software update completed successfully • **S_watson_AUTOMATIC_SWUPDATE_ABORTED** Software update aborted • **S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE** Software update aborted due to an incorrect device software image • **S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE** Software update aborted because the device did not save the device software image.

Configuring the Ports

The following port configuration functions are available:

- Enabling/Disabling the port
- Selecting the operating mode
- Gigabit Ethernet mode for ports

Enabling/Disabling the Port

In the default setting, every port is enabled. For a greater level of access security, disable unconnected ports. To do this, perform the following steps:

Step	Action
1	Navigate to the **Basic Settings > Port**, **Configuration** tab.
2	To enable a port, select the checkbox in the Port on column.
3	To disable a port, clear the checkbox in the Port on column.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`no shutdown`	To enable the interface.

Selecting the Operating Mode

In the default setting, the ports are set to Autoneg operating mode.

> **NOTE:** The active automatic configuration has priority over the manual configuration.

Perform the following steps:

Step	Action
1	Navigate to the **Basic Settings > Port**, **Configuration** tab.
2	If the device connected to this port requires a fixed setting, perform the following steps: • Deactivate the function. Clear the checkbox in the Autoneg column. • In the Manual configuration column, specify the desired operating mode (transmission rate, duplex mode).
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`no auto-negotiate`	To disable the automatic configuration mode.
`speed 100 full`	To set port speed 100 Mbit/s and full-duplex.

Gigabit Ethernet Mode for Ports

The device supports 2.5 Gbit/s on several interfaces with one of the following SFP transceivers:

- M-SFP-2.5-MM/LC EEC
- M-SFP-2.5-SM-/LC EEC
- M-SFP-2.5-SM/LC EEC
- M-SFP-2.5-SM+/LC EEC

The type of the transceiver plugged into the slot determines the port speed. The device has no option to set the speed manually. Ports with 2.5 Gbit/s speed only support data rates of 1 Gbit/s and greater.

Depending on the hardware of the device, the actual usable data rate might be lower than the data rate that the media module supports.

> **NOTE:** For further information about the transceiver references, see the *Accessories* chapter in the *Modicon MCSESM, MCSESP Series Managed Switch Installation Guide*.

Port Parameters Verification

You use the Gigabit Ethernet mode to get a greater bandwidth for uplinks. To use this function, insert an applicable transceiver type in the appropriate slot.

Perform the following step:

- Navigate to the **Basic Settings > Port**, **Configuration** tab.

  The column Manual configuration displays the value **2.5 Gbit/s FDX** for the ports that have a 2.5 Gbit/s SFP transceiver inserted.

  You cannot change the speed.

Perform the following commands:

Command	Description
`show port 1/1`	To display the parameters for slot **1** port **1**. The `Physical Mode` list entry displays the value `2500 full` for the ports that have a 2.5 Gbit/s SFP transceiver inserted.

```
Interface....................1/1
Name.........................My interface
--
Cable-crossing Setting........-
Physical Mode................2500 full
Physical Status...............-
```

Assistance in the Protection From Unauthorized Access

The device offers functions that help you protect the device against unauthorized access.

After you set up the device, carry out the following steps to reduce possible unauthorized access to the device:

- Changing the SNMPv1/v2 community
- Disabling write access for SNMPv1/v2
- Disabling SNMPv1/v2
- Disabling HTTP
- Using your own HTTPS certificate
- Using your own SSH key
- Disabling Telnet
- Disabling Ethernet Switch Configurator
- Restricting access to device management
- Adjusting the session timeouts
- Customizing the SSH settings
- Making SSH hosts defined by the device

Changing the SNMPv1/v2 Community

SNMPv1 and SNMPv2 work unencrypted. Every SNMP packet contains the IP address of the sender and the plaintext *community name* with which the sender accesses the device. If the SNMPv1 and/or SNMPv2 function is active, the device allows anyone who knows the *community name* to access the device. Treat the *community names* with discretion.

The *community names* **user** for *read-only* access and **admin** for *read and write* access are preset. If you are using SNMPv1 or SNMPv2, change the default *community name*. To do this, perform the following steps:

Step	Action
1	Navigate to **Device Security > Management Access > SNMPv1/v2 Community**. The dialog displays the communities that are set up.
2	For the **Write** community, specify the *community name* in the **Name** column: • Up to 64 alphanumeric characters are permitted. • The device differentiates between upper and lowercase. • Specify a different *community name* than for *read-only* access.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp community rw <community name>`	To specify the community for *read and write* access.
`show snmp community`	To display the communities that have been set up.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Disabling Write Access for SNMPv1/v2

To reduce possible unauthorized access to the device, you can disable the write access for the **Write** community, while the *read-only* access remains enabled. To do this, perform the following steps:

Step	Action
1	Navigate to the **Device Security > Management Access > SNMPv1/v2 Community**, **Configuration** tab.
2	Deactivate the write access for the **Write** community. To do this, select the SNMP V1/V2 readOnly checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp community rw private read-only`	To deactivate the write access for the **admin** community.
`show snmp community`	To display the SNMP access mode of the SNMPv1/v2 communities.

`SNMP V1/V2 community`
`--------------------`
`public`
`private`
	`Access mode`
	`-----------`
	`read-only`
	`read-only`

`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Disabling SNMPv1/v2

If you need SNMPv1 or SNMPv2, use these protocols only in environments protected from eavesdropping. SNMPv1 and SNMPv2 do not use encryption. The SNMP packets contain the community in clear text. Use, if possible, SNMPv3 in the device and disable access using SNMPv1 and SNMPv2. To do this, perform the following steps:

Step	Action
1	Navigate to the **Device Security** **>** **Management Access** **>** **Server**, **SNMP** tab. The dialog displays the settings of the SNMP server.
2	To deactivate the SNMPv1 protocol, clear the SNMPv1 checkbox.
3	To deactivate the SNMPv2 protocol, clear the SNMPv2 checkbox.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no snmp access version v1`	To deactivate the SNMPv1 protocol.
`no snmp access version v2`	To deactivate the SNMPv2 protocol.
`show snmp access`	To display the SNMP server settings.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Disabling HTTP

The web server provides the Graphical User Interface with the protocol HTTP or HTTPS. HTTPS connections are encrypted, while HTTP connections are unencrypted.

The HTTP protocol is enabled by default. If you disable HTTP, no unencrypted access to the Graphical User Interface is possible. To do this, perform the following steps:

Step	Action
1	Navigate to the **Device Security** **>** **Management Access** **>** **Server**, **HTTP** tab.
2	Disable the HTTP protocol. Select the **Off** radio button in the Operation frame.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no http server`	To disable the HTTP protocol.

If the HTTP protocol is disabled, you can reach the Graphical User Interface of the device only by HTTPS. In the address bar of the web browser, enter the string https:// before the IP address of the device.

If the HTTPS protocol is disabled and you also disable HTTP, the Graphical User Interface is unaccessible. To work with the Graphical User Interface, enable the HTTPS server using the Command Line Interface. To do this, execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`https server`	To enable the HTTPS protocol.

Disabling Telnet

The device allows remote access to the device management using Telnet or SSH. Telnet connections are unencrypted, while SSH connections are encrypted.

The Telnet server is enabled in the device by default. If you disable Telnet, unencrypted remote access to the Command Line Interface is no longer possible. To do this, perform the following steps:

Step	Action
1	Navigate to the **Device Security > Management Access > Server**, **Telnet** tab.
2	Disable the Telnet server. Select the **Off** radio button in the Operation frame.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no telnet server`	To disable the Telnet server.

If the SSH server is disabled and you also disable the Telnet server, access to the device management is only possible using the Command Line Interface through the serial connection. To work remotely with the Command Line Interface, enable SSH. To do this, perform the following steps:

Step	Action
1	Navigate to the **Device Security > Management Access > Server**, **SSH** tab.
2	Enable the SSH server. Select the **On** radio button in the Operation frame.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh server`	To enable the SSH server.

Disabling the Ethernet Switch Configurator Access

Ethernet Switch Configurator allows assignment of IP parameters to the device over the network during commissioning. Ethernet Switch Configurator communicates in the device management VLAN without encryption and authentication.

After the device is commissioned, set Ethernet Switch Configurator to read-only or disable Ethernet Switch Configurator access completely. To do this, perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Network > Global**.
2	To take away write permission from the Ethernet Switch Configurator software, in the Ethernet Switch Configurator protocol v1/v2 frame, specify the value **readOnly** in the **Access** field.
3	Disable Ethernet Switch Configurator access completely. Select the **Off** radio button in the Ethernet Switch Configurator protocol v1/ v2 frame.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`network ethernet-switch-conf mode read-only`	To disable write permission of the Ethernet Switch Configurator software.
`no network ethernet-switch-conf operation`	To disable Ethernet Switch Configurator access.

Restricting Access to Device Management

In the default setting, everyone can access the device management from any IP address using any protocol. The device allows access to be restricted to device management for selected protocols from a specific IP address range.

Restricting Access from a Specific IP Address Range

In the following example, the device is to be accessible only from the company network using the Graphical User Interface. The administrator has additional remote access using SSH. The company network has the address range **192.168.1.0/24** and remote access from a mobile network with the IP address range **109.237.176.0/24**. The SSH application program the fingerprint of the RSA key.

The following table presents parameters for the IP access restriction:

Parameter	Company network	Mobile phone network
Network address	**192.168.1.0**	**109.237.176.0**
Netmask	**24**	**24**
Desired protocols	https, snmp	ssh

Perform the following steps:

Step	Action
1	Navigate to **Device Security > Management Access > IP Access Restriction**.
2	Clear the checkbox in the Active column for the table row. This entry allows users access to the device from any IP address and the supported protocols.
3	Address range of the company network:
4	To add a table row, click the + button.
5	Specify the address range of the company network in the IP address range column: **192.168.1.0/24**
6	For the address range of the corporate network, deactivate the undesired protocols. The HTTPS, SNMP, and Active checkboxes remain selected.
7	Address range of the mobile phone network:
8	To add a table row, click the + button.
9	Specify the address range of the mobile network in the IP address range column: **109.237.176.0/24**
10	For the address range of the mobile network, deactivate the undesired protocols. The SSH and Active checkboxes remain selected.
11	Enable the access restriction. Select the **On** radio button in the Operation frame. **NOTE:** Before you enable the access restriction, verify that the table contains at least one active rule that grants you access to the device management. Otherwise, access to the device management is only possible using the Command Line Interface through the serial connection.
12	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`show network management access global`	To display if the access restriction is enabled or disabled.
`show network management access rules`	To display the entries that have been configured.
`no network management access operation`	To disable the IP access restriction.
`network management access add 2`	To add a rule with index `2` for the address range of the company network.
`network management access modify 2 ip 192.168.1.0`	To specify the IP address of the company network.
`network management access modify 2 mask 24`	To specify the netmask of the company network.
`network management access modify 2 ssh disable`	To deactivate SSH for the address range of the company network. Repeat the operation for every unwanted protocol.
`network management access add 3`	To add a rule with index `3` for the address range of the mobile phone network.
`network management access modify 3 ip 109.237.176.0`	To specify the IP address of the mobile phone network.
`network management access modify 3 mask 24`	To specify the netmask of the mobile phone network.
`network management access modify 3 snmp disable`	To deactivate SNMP for the address range of the mobile phone network. Repeat the operation for every unwanted protocol.
`no network management access status 1`	To deactivate the default entry. This entry allows users access to the device from any IP address and the supported protocols.
`network management access status 2`	To activate the rule with index `2` for the address range of the company network.
`network management access status 3`	To activate the rule with index `3` for the address range of the mobile phone network.
`show network management access rules`	To display the entries that have been configured.
`network management access operation`	To enable the access restriction.

Adjusting the Session Timeouts

The device allows automatic termination of the session upon inactivity of the user that is logged in. The session timeout is the period of inactivity after the last user action.

You can specify a session timeout for the following applications:

- Command Line Interface sessions using an SSH connection
- Command Line Interface sessions using a Telnet connection
- Command Line Interface sessions using the serial connection
- Graphical User Interface

Timeout for Command Line Interface Sessions Using a SSH connection

Perform the following steps:

Step	Action
1	Navigate to the **Device Security > Management Access > Server**, **SSH** tab.
2	Specify the timeout period in minutes in the **Configuration frame, Session timeout [min]** field.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh timeout <0..160>`	To specify the timeout period in minutes for Command Line Interface sessions using an SSH connection.

Timeout for Command Line Interface Sessions Using a Telnet Connection

Perform the following steps:

Step	Action
1	Navigate to the **Device Security > Management Access > Server**, **Telnet** tab.
2	Specify the timeout period in minutes in the **Configuration frame, Session timeout [min]** field.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`telnet timeout <0..160>`	To specify the timeout period in minutes for Command Line Interface sessions using a Telnet connection.

Timeout for Command Line Interface Sessions Using the Serial Connection

Perform the following steps:

Step	Action
1	Navigate to the **Device Security > Management Access > CLI**, **Global** tab.
2	Specify the timeout period in minutes in the Configuration frame, **Serial interface timeout (min)** field.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`cli serial-timeout <0..160>`	To specify the timeout period in minutes for Command Line Interface sessions using the serial connection.

Session Timeout for the Graphical User Interface

Perform the following steps:

Step	Action
1	Navigate to **Device Security > Management Access > Web**.
2	Specify the timeout period in minutes in the Configuration frame, **Web interface session timeout [min]** field.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`network management access web timeout <0..160>`	To specify the timeout period in minutes for Graphical User Interface sessions

Command	Description

Customizing the SSH Settings

In the state on delivery, the built-in SSH server of the device uses a self-signed RSA *host key*. To increase the security level of SSH connections to the device, you can replace the RSA *host key* in the device in the following ways:

- Generating the RSA Host Key in the Device, page 117
- Transferring an Externally Generated Private RSA Key to the Device, page 117

Generating the RSA *host key* in the Device

The device allows generation of an RSA *host key* directly in the device and thus replace the stored RSA *host key*. To do this, perform the following steps:

Step	Action
1	Navigate to the **Device Security > Management Access > Server**, **SSH** tab.
2	Disable the SSH server. To do this, in the Operation frame, select the **Off** radio button.
3	To apply the settings, click the ✓ button.
4	In the Signature frame, click **Create**. Generating the new RSA *host key* starts. You can monitor the process when you click the ⟳ button. When the value in the **Oper status** field changes from **rsa** to **none**, the process is complete.
5	Enable the SSH server. To do this, in the Operation frame, select the **On** radio button. The generated RSA *host key* is immediately active.
6	To apply the settings, click the ✓ button.

Execute the following commands only if you are connected to the device management through the serial connection. If you are connected through SSH, the connection to the device management will be lost:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no ssh server`	To disable the SSH server.
`ssh key rsa generate`	To generate the new RSA *host key*. This process takes a few seconds and finishes without feedback. You can monitor the process when you execute the `show ssh server` command. When the value in the `SSH key operation status` line changes from `rsa` to `none`, the process is complete.
`ssh server`	To enable the SSH server. The generated RSA *host key* is immediately active.

Transferring an Externally Generated Private RSA Key to the Device

Network administrators can generate an RSA *host key* outside the device, for example, by using the `ssh-keygen` command, which is part of OpenSSH. Optionally, you can have the externally generated RSA key signed by a Certification Authority (CA).

To generate an RSA key outside the device, enter the following command on the PC: `ssh-keygen -b 2048 -t rsa -m PEM -N '' -f key_name`

- `-b 2048`

  Length of the key
- `-t rsa`

  Type of the key
- `-m PEM`

  Format of the key
- `-N ''`

  Passphrase
- `-f key_name`

  File name of the key

  Replace the string `key_name` with the desired file name.

After the command has completed, you find the following files in the file system of the PC:

- Private key (`key_name` without file extension)

  This key enables the SSH server in the device to authenticate itself to the SSH clients. You transfer this key to the device in the further process. Keep the private key in a trusted, secure location, but not in a publicly accessible or shared location.
- Public key (`key_name` with the file extension .pub)

  This key enables SSH clients to verify the authenticity of the SSH server in the device.

You can transfer the externally generated private key to the device using one of the following options:

- Importing the private key from the PC or a file server directly into the device using the Graphical User Interface or the Command Line Interface.

  Importing the Private Key Directly Into the Device, page 118
- Transferring the private key to the device through the external memory using the Command Line Interface.

  Transferring the Private Key to the Device Through the External Memory, page 120

Importing the Private Key Directly Into the Device

You can import the private key from the PC or a file server directly into the device using the Graphical User Interface or Command Line Interface. Confirm that the private key resides on the file server for the shortest time necessary during the transfer. Immediately after the transfer, relocate the private key to a location that is inaccessible from the network.

Perform the following steps:

Step	Action
1	Navigate to the **Device Security > Management Access > Server**, **SSH** tab.
2	Disable the SSH server. To do this, in the Operation frame, select the **Off** radio button.
3	To apply the settings, click the ✓ button.
4	Import the private key: • When the file is located on your PC or on a network drive, drag and drop it onto the ⇧ area. As an alternative, click in the area to select the file. • If the file is on an FTP server, specify the URL in the following form: ftp://<user>:<password>@<IP address>[:port]/<file name> Do not use this method if you transmit data over untrusted networks. • If the file is on a TFTP server, specify the URL in the following form: tftp://<IP address>/<path>/<file name> Do not use this method if you transmit data over untrusted networks. • If the file is on an SCP or SFTP server, specify the URL in one of the following forms: scp:// or sftp://<IP address>/<path>/<file name> When you click **Start**, the device displays the Credentials window. There you enter User name and Password to log into the server. scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name> Ensure that the SCP or SFTP server is defined by the device before the device accesses the server for the first time. See the **Device Security > SSH Known Hosts** dialog.
5	Click **Start**. The file transfer starts. This process takes a few seconds.
6	Relocate the private key to a location that is inaccessible from the network.
7	Enable the SSH server. To do this, in the Operation frame, select the **On** radio button. The imported private key is immediately active.
8	To apply the settings, click the ✓ button.

Execute the following commands only if you are connected to the device management through the serial connection. If you are connected through SSH, the connection to the device management will be lost:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`copy sshkey remote scp://192.168.1.1/path/to/priv_key_file nvm`	To import the private key from a PC with the IP address 192.168.1.1 using SCP. Immediately after the transfer, relocate the private key to a location that is inaccessible from the network.
`configure`	To change to the Configuration mode.
`no ssh server`	To disable the SSH server.
`ssh server`	To enable the SSH server. The imported private key is immediately active.

Transferring the Private Key to the Device Through the External Memory

You can transfer the private key to the device through the external memory using the Command Line Interface.

Preparatory steps:

- On the PC, copy the private key to the external memory connected to the PC. Confirm that the private key resides on the external memory for the shortest time necessary during the transfer. Immediately after the transfer, wipe the private key from the external memory.
- Plug the external memory into the device.

Execute the following commands only if you are connected to the device management through the serial connection. If you are connected through SSH, the connection to the device management will be lost:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`copy sshkey envm path/to/priv_key_file nvm`	To transfer the private key to the device through the external memory (**ENVM**). Immediately after the transfer, wipe the private key from the external memory (**ENVM**).
`configure`	To change to the Configuration mode.
`no ssh server`	To disable the SSH server.
`ssh server`	To enable the SSH server. The imported private key is immediately active.

Making SSH Hosts Defined by the Device

The device permits SSH-based connections only to remote servers that are defined by the device. In the state on delivery, no remote server is a defined host on the device.

When downloading a device software image or importing a configuration profile from an SCP or SFTP server, these protocols use an underlying SSH connection. For SSH, define remote servers by using their public key fingerprint. The device verifies the identity of the remote server by comparing the public key fingerprint stored on the device with the fingerprint calculated from the public key which the remote server actually sent. If the calculated public key fingerprint does not match the stored public key fingerprint, the device terminates the connection.

You can find out the public key fingerprint of the remote server and the key type, as follows:

- From the administrator of a defined SSH server.

  Use a trustworthy channel for receiving this data.
- From the error message following an unsuccessful software update in the Software dialog.

  This happens because of the mismatch between the public key fingerprint stored in the device and the fingerprint calculated from the public key which the remote server actually sent.

The device provides the following setting options:

- Adding an SSH-Defined Hosts Entry, page 121
- Updating an SSH-Defined Hosts Entry, page 121
- Deactivating an SSH-Defined Hosts Entry, page 122
- Deleting an SSH Defined-Hosts Entry, page 123

Adding an SSH-Defined Host Entry

You can set up a maximum of 50 entries containing the server address and the public key fingerprint. If a remote server has several keys set up, for different encryption algorithms, add each of the public key fingerprints as a separate entry.

Verify that the public key fingerprints you store on the device are from a trustworthy source, the SSH server administrator, for example.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Port**.
2	Click the + button. The dialog displays the Create window.
3	In the **Index** field, specify the index value. Assign a unique value.
4	In the **Address** field, specify the IPv4 or IPv6 address, or the DNS hostname of the remote server.
5	In the **Key fingerprint** field, enter the public key fingerprint of the remote server.
6	From the Key type drop-down list, select the corresponding key type. This is the algorithm that the administrator of the remote server used to generate the server key pair.
7	Click **OK**. The device adds a table row. The device accepts establishing a connection to the remote server from now on.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh known-hosts add {index} address {ipv4 | ipv6 | dns} key-type {rsa | dsa | ecdsa | ed25519} key-fingerprint {string_base64}`	To add an entry with index, address of the remote server, key type, and public key fingerprint of the remote server.
`show ssh known-hosts`	To display the set up entries.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, refer to Saving a Configuration Profile, page 87.

Updating an SSH-Defined Host Entry

If the public key of the remote server changes, you need to update the fingerprint in the respective table row.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings** **>** **Port**.
2	• Clear the checkbox in the Active column. • To apply the settings, click the ✓ button.
3	• In the Key fingerprint column, enter the new public key fingerprint of the remote server. • To apply the settings, click the ✓ button.
4	To activate the entry, select the checkbox in the Active column.
5	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh known-hosts modify {index} status disable`	To deactivate the entry.
`ssh known-hosts modify {index} key-fingerprint {string_base64}`	To modify the entry with the index number you have entered.
`ssh known-hosts modify {index} status enable`	To activate the entry.
`show ssh known-hosts {index}`	To verify the updated entry.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, refer to Saving a Configuration Profile, page 87.

Deactivating an SSH-Defined Host Entry

You deactivate an entry, for example, when the present server key will soon become invalid due to the rotation of the server key.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings** **>** **Port**.
2	In the table row for the relevant entry, clear the checkbox in the Active column.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh known-hosts modify {index} status disable`	To deactivate the entry with the index number you have entered.
`show ssh known-hosts {index}`	To verify if the entry is inactive.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, refer to Saving a Configuration Profile, page 87.

Deleting an SSH Known Hosts Entry

If the device is no longer permitted to contact a remote server or the public key is no longer valid, you can delete the corresponding entry.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Port**.
2	In the table row for the relevant entry, select the checkbox in the Index column. Click the ✖ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh known-hosts delete {index}`	To delete the entry with the index number you have entered.
`show ssh known-hosts {index}`	To verify if the entry has been deleted.

`SSH known hosts information`
`---------------------------`
`No entry.`
	–

`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, see Saving a Configuration Profile, page 87.

Controlling the Data Traffic

The device verifies the data packets to be forwarded in accordance with defined rules. Data packets to which the rules apply are either forwarded by the device or blocked. If data packets do not correspond to any of the rules, the device blocks the packets.

Routing ports to which no rules are assigned allow packets to pass through. As soon as a rule is assigned, the assigned rules are processed first. After that, the specified standard action of the device takes effect.

The device provides the following functions for controlling the data stream:

- Service request control (Denial of Service (DoS))
- Denying access to devices based on their IP or MAC address (ACL)

The device observes and monitors the data stream. The device takes the results of the observation and the monitoring and combines them with the rules for the network security to generate a status table. Based on this status table, the device determines whether to accept, drop or reject data.

The data packets go through the filter functions of the device in the following sequence:

- DoS … if **permit** or **accept**, then progress to the next rule
- ACL … if **permit** or **accept**, then progress to the next rule

Helping Protect Against DoS Attacks

Denial of Service (DoS) is a cyberattack that aims to make certain services or devices unusable. Attackers as well as network administrators can use the port scan method to discover open ports in a network to find vulnerable devices. The function helps you protect the network against invalid or falsified data packets targeted at certain services or devices. You have the option of specifying filters to help restrict the data stream for protection against DoS attacks. The filters verify the received data packets. The device discards a data packet if it matches the filter criteria.

To help protect the device and other devices in the network from DoS attacks, the device allows the following options:

- Filters for TCP and UDP Packets, page 125
- Filters for IP Packets, page 128
- Filters for ICMP Packets, page 129

The filters help prevent an attacking station from:

- Detecting services and applications that use the open ports
- Detecting active devices in a network
- Accessing sensitive data in a network
- Detecting active security devices like a firewall used in a network

  NOTE: You can combine the filters in any way. When you activate several filters, the device applies the filters in the order in which they are specified in the IP table. If an incoming data packet matches a filter, the device discards the respective data packet and then stops further processing.

Filters for *TCP* and *UDP* Packets

To selectively process *TCP* and *UDP* packets, the device offers you the following filters:

- Activating the Null Scan Filter Function, page 125
- Activating the Xmas Filter Function, page 125
- Activating the SYN/FIN Filter Function, page 126
- Activating the TCP Offset Protection Function, page 126
- Activating the TCP SYN Protection Function, page 127
- Activating the L4 Port Protection Function, page 127

Activating the Null Scan Filter Function

With the *Null Scan* method, the attacking station sends data packets with the following properties:

- No *TCP* flags are set.
- The *TCP* sequence number is 0.

The device uses the Null Scan filter function to discard incoming *TCP* packets that contain malicious properties.

In the default setting, the Null Scan filter function is disabled. To activate the Null Scan filter function, perform the following steps:

Step	Action
1	Navigate to **Network Security > DoS > Global**.
2	Activate the Null Scan filter function. To do this, in the TCP/UDP frame, select the Null Scan filter checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos tcp-null`	To activate the Null Scan filter function.
`no dos tcp-null`	To deactivate the Null Scan filter function.

Activating the Xmas Filter Function

With the *Xmas* method, the attacking station sends data packets with the following properties:

- The *TCP* flags *FIN*, *URG*, and *PSH* are simultaneously set.
- The *TCP* sequence number is 0.

The device uses the Xmas filter function to discard incoming *TCP* packets that contain malicious properties.

In the default setting, the Xmas filter function is disabled. To activate the Xmas filter function, perform the following steps:

Step	Action
1	Navigate to **Network Security > DoS > Global**.
2	Activate the Xmas filter function. To do this, in the TCP/UDP frame, select the Xmas filter checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos tcp-xmas`	To activate the Xmas filter function.
`no dos tcp-xmas`	To deactivate the Xmas filter function.

Activating the SYN/FIN Filter Function

With the *SYN/FIN* method, the attacking station sends data packets with the *TCP* flags *SYN* and *FIN* set simultaneously. The device uses the SYN/FIN filter function to discard incoming packets with the *TCP* flags *SYN* and *FIN* set simultaneously.

In the default setting, the SYN/FIN filter function is disabled. To activate the SYN/FIN filter function, perform the following steps:

Step	Action
1	Navigate to **Network Security > DoS > Global**.
2	Activate the SYN/FIN filter function. To do this, in the TCP/UDP frame, select the SYN/FIN filter checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos tcp-syn-fin`	To activate the SYN/FIN filter function.
`no dos tcp-syn-fin`	To deactivate the SYN/FIN filter function.

Activating the TCP Offset Protection Function

With the *TCP Offset* method, the attacking station sends data packets whose fragment offset is equal to **1**. The fragment offset is a field in the *IP* header which helps to identify the sequence of fragments in received data packets. The device uses the TCP Offset protection function to discard incoming *TCP* data packets whose fragment offset field in the *IP* header is equal to **1**.

NOTE: The device accepts *UDP* and *ICMP* packets whose fragment offset field of the *IP* header is equal to **1**.

In the default setting, the TCP Offset protection function is disabled. To activate the TCP Offset protection function, perform the following steps:

Step	Action
1	Navigate to **Network Security > DoS > Global**.
2	Activate the TCP Offset protection function. To do this, in the TCP/UDP frame, select the TCP Offset protection checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos tcp-offset`	To activate the TCP Offset protection function.
`no dos tcp-offset`	To deactivate the TCP Offset protection function.

Activating the TCP SYN Protection Function

With the *TCP SYN* method, the attacking station sends data packets with the *TCP* flag *SYN* set and an L4 (layer 4) source port <1024. The device uses the TCP SYN protection function to discard incoming packets with the *TCP* flag *SYN* set and an L4 (layer 4) source port <1024.

In the default setting, the TCP SYN protection function is disabled. To activate the TCP SYN protection function, perform the following steps:

Step	Action
1	Navigate to **Network Security > DoS > Global**.
2	Activate the TCP SYN protection function. To do this, in the TCP/UDP frame, select the TCP SYN protection checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos tcp-syn`	To activate the TCP SYN protection function.
`no dos tcp-syn`	To deactivate the TCP SYN protection function.

Activating the L4 Port Protection Function

An attacking station can send *TCP* or *UDP* data packets whose source port number and destination port number are identical. The device uses the L4 Port protection function to discard incoming *TCP* and *UDP* packets whose L4 source port and destination port number are identical.

In the default setting, the L4 Port protection function is disabled. To activate the L4 Port protection function, perform the following steps:

Step	Action
1	Navigate to **Network Security > DoS > Global**.
2	Activate the L4 Port protection function. To do this, in the TCP/UDP frame, select the L4 Port protection checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos l4-port`	To activate the L4 Port protection function.
`no dos l4-port`	To deactivate the L4 Port protection function.

Filters for *IP* Packets

To selectively process *IP* packets, the device offers you the following filters:

- Activating the Land Attack Filter Function, page 128

Activating the Land Attack Filter Function

With the *Land Attack* method, the attacking station sends data packets whose source and destination addresses are identical to the *IP* address of the recipient. The device uses the Land Attack filter function to discard received packets whose source and destination addresses are identical.

In the default setting, the Land Attack filter function is disabled. To activate the Land Attack filter function, perform the following steps:

Step	Action
1	Navigate to **Network Security > DoS > Global**.
2	Activate the Land Attack filter function. To do this, in the IP frame, select the Land Attack filter checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos ip-land enable`	To activate the Land Attack filter function.
`no dos ip-land disable`	To deactivate the Land Attack filter function.

Filters for *ICMP* Packets

To selectively process *ICMP* packets, the device offers you the following filters:

- Activating the Fragmented Packets Filter Function, page 129
- Activating the Packet Size Filter Function, page 129
- Activating the Drop Broadcast Ping Function, page 130

Activating the Fragmented Packets Filter Function

The device uses the Fragmented packets filter function to help protect the network from attacking stations that send fragmented *ICMP* packets. Fragmented *ICMP* packets can cause the destination device to be inoperable if the destination device processes fragmented *ICMP* packets incorrectly. The device uses the Fragmented packets filter function to discard fragmented *ICMP* packets.

In the default setting, the Fragmented packets filter function is disabled. To activate the Fragmented packets filter function, perform the following steps:

Step	Action
1	Navigate to **Network Security > DoS > Global**.
2	Activate the Fragmented packets filter function. To do this, in the ICMP frame, select the Fragmented packets filter checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos icmp-fragmented`	To activate the Fragmented packets filter function.
`no dos icmp-fragmented`	To deactivate the Fragmented packets filter function.

Activating the Packet Size Filter Function

The device uses the Packet size filter to discard data packets whose payload size exceeds the size specified in the **Allowed payload size [byte]** field.

The Packet size filter function helps protect the network from attacking stations that send *ICMP* packets whose payload size exceeds the size specified in the **Allowed payload size [byte]** field.

In the default setting, the Packet size filter function is disabled. To activate the Packet size filter function, perform the following steps:

Step	Action
1	Navigate to **Network Security > DoS > Global**.
2	Activate the Packet size filter function. To do this, in the ICMP frame, select the Packet size filter checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos icmp payload-check`	To activate the Packet size filter function.
`no dos icmp payload-check`	To deactivate the Packet size filter function.

Activating the Drop Broadcast Ping Function

The Drop broadcast ping function helps protect the network from broadcast ping attacks, also known as ICMP Smurf attacks. With the broadcast ping method, the attacker floods a target device (the victim) by sending a large number of *ICMP echo request* packets to the IPv4 broadcast address. These packets contain a spoofed IP source address which is the IP address of the victim. Stations responding to the broadcast ping send their replies to the victim, thus flooding the victim and possibly causing instability.

The device uses the Drop broadcast ping function to discard the broadcast pings.

In the default setting, the Drop broadcast ping function is disabled. To activate the Drop broadcast ping function, perform the following steps:

Step	Action
1	Navigate to **Network Security > DoS > Global**.
2	Activate the Drop broadcast ping function. To do this, in the ICMP frame, select the Drop broadcast ping checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dos icmp-smurf-attack`	To activate the Drop broadcast ping function.
`no dos icmp-smurf-attack`	To deactivate the Drop broadcast ping function.

ACL

In this menu you can enter the parameters for the Access Control Lists (ACLs).

The device uses ACLs to filter data packets received on VLANs or on individual or multiple ports. In a ACL, you specify rules that the device uses to filter data packets. When such a rule applies to a packet, the device applies the actions specified in the rule to the packet.

The following actions are available:

- Allow (**permit**)
- Discard (**deny**)
- Redirect to a certain port (see Redirection port field)
- Mirror (see Mirror port field)

You can apply the following criteria in order to filter the data packets:

- Source or destination address of a packet (MAC)
- Source or destination address of a data packet (IPv4)
- Type of the transmitting protocol (MAC/IPv4)
- Source or destination port of a data packet (IPv4)
- Service class of a packet (MAC)
- Membership of a specific VLAN (MAC)
- DSCP classification (IPv4)
- ToS classification (IPv4)
- Packet Fragmentation (IPv4)

You can specify the following ACL types:

- IP ACLs for VLANs
- IP ACLs for ports
- MAC ACLs for VLANs
- MAC ACLs for ports

When you assign both an IP ACL and MAC ACL to the same interface, the device first uses the IP ACL to filter the data stream. The device applies the MAC ACL rules only after the packets are filtered through the IP ACL. The priority of an ACL is independent of the index of a rule.

Within an ACL, the device processes the rules in order. The index of the respective rule determines the order in which the device filters the data stream. When you assign an ACL to a port or VLAN, you can specify its priority with the index. The lower the number, the greater the priority. The device processes the rule with the greater priority first.

If none of the rules specified in an ACL applies to a data packet, the implicit **deny** rule applies. As a result, the device drops the received data packets.

Keep in mind that the device directly implements the implicit **deny** rule.

NOTE: The number of available ACLs depends on the device. For further information about the ACL values, refer to chapter Technical Data, page 387.

NOTE: You can assign a single ACL to any number of ports or VLANs.

NOTE: If you activate the Packet fragmented function for a rule, the rule processes IPv4 fragments with the offset other than zero. The rule processes every IPv4 fragment except for the initial IPv4 fragment.

The ACL menu contains the following dialogs:

- IPv4 Rule
- MAC Rule
- Assignment

These dialogs provide the following options:

- To specify the rules for the various ACL types.
- To provide the rules with the required priorities.
- To assign the ACLs to ports or VLANs.

Creating and Editing IPv4 Rules

When filtering IPv4 data packets, the device allows the following:

- Add new groups and rules
- Add new rules to existing groups
- Edit an existing rule
- Activate and deactivate groups and rules
- Delete existing groups and rules
- Change the order of existing rules

Perform the following steps:

Step	Action
1	Navigate to **Network Security** > **ACL** > **IPv4 Rule**.
2	Click the + button. The dialog displays the Create window.
3	Click the Group name drop-down list to specify the ACL (group) name. Enter the name in the search box. • To use an existing name, select the desired item from the search results. • To add a name, click the **Create** link below the search box.
4	In the **Index** field you specify the number for the rule within the ACL. This number defines the priority of the rule.
5	Click **OK**. The device adds the rule to the ACL (group) in the table. The rule is active immediately. To remove a rule, select the desired table row and click the ✕ button.
6	Edit the rule parameters in the table. To change a value, double-click the relevant field.
7	To apply the settings, click the ✓ button.

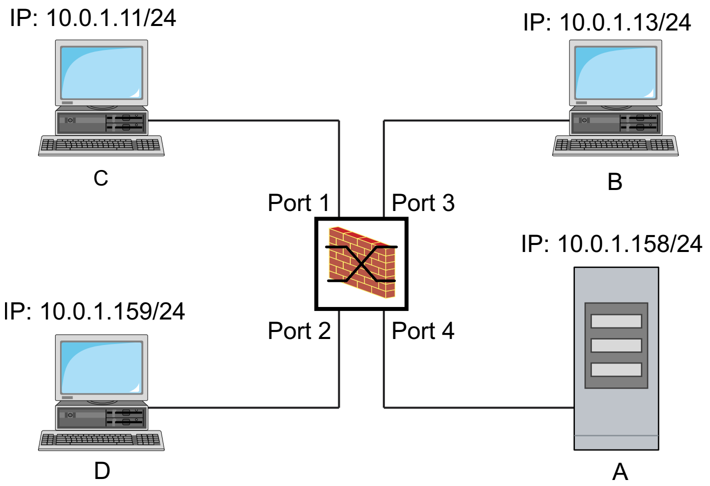
NOTE: The device allows wildcards with the Source IP address and Destination IP address parameters. If you enter for example, **192.168.?.?**, the device allows addresses that start with **192.168**.

NOTE: The prerequisite for changing the values in the Source TCP/UDP port and Destination TCP/UDP port column is that you specify the value **tcp** or **udp** in the Protocol column.

NOTE: The prerequisite for changing the value in the Redirection port and Mirror port column is that you specify the value **permit** in the Action column.

Creating and Configuring an IP ACL Using the Command Line Interface

In the following example, you set up ACLs to block the communication from computers B and C to computer A, based on the IP address (TCP/UDP port, etc.):



Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ip access-list extended name filter1 deny src 10.0.1.11-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	To add an IP ACL with name `filter1`. To add a rule denying IP data packets from `10.0.1.11` to `10.0.1.158`. Priority `1` (highest priority).
`ip access-list extended name filter1 permit src any dst any`	To add a rule to the IP ACL admitting IP data packets.
`show access-list ip filter1`	To display the rules of the IP ACL `filter1`.
`ip access-list extended name filter2 deny src 10.0.1.13-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	To add an IP ACL with name `filter2`. To add a rule denying IP data packets from `10.0.1.13` to `10.0.1.158`. Priority `1` (highest priority).
`show access-list ip filter2`	To display the rules of the IP ACL `filter2`.

Creating and Editing MAC Rules

When filtering MAC data packets, the device allows to:

- Add new groups and rules
- Add new rules to existing groups
- Edit an existing rule
- Activate and deactivate groups and rules
- Delete existing groups and rules
- Change the order of existing rules

Perform the following steps:

Step	Action
1	Navigate to **Network Security > ACL > MAC Rule**.
2	Click the + button. The dialog displays the Create window.
3	Click the Group name drop-down list to specify the ACL (group) name. Enter the name in the search box. • To use an existing name, select the desired item from the search results. • To add a name, click the **Create** link below the search box.
4	In the **Index** field you specify the number for the rule within the ACL. This number defines the priority of the rule.
5	Click **OK**. The device adds the rule to the ACL (group) in the table. The rule is active immediately. To remove a rule, select the desired table row and click the × button.
6	Edit the rule parameters in the table. To change a value, double-click the relevant field.
7	To apply the settings, click the ✓ button.

NOTE: In the Source MAC address and Destination **MAC address** fields you can use wildcards in the **FF:??:??:??:??:??** or **??:??:??:??:00:01** form. Use capital letters here.

Creating and Configuring a MAC ACL Using the Command Line Interface

In the following example, AppleTalk and IPX are to be filtered out from the entire network. To do this, execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mac acl add 1 macfilter`	To add an MAC ACL with the ID **1** and the name **macfilter**.
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	To add a rule to position **1** of the MAC ACL with the ID **1** rejecting packets with EtherType **0x809B (AppleTalk)**.
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	To add a rule to position **2** of the MAC ACL with the ID **1** rejecting packets with EtherType **0x8137 (IPX alt)**.
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	To add a rule to position **3** of the MAC ACL with the ID **1** rejecting packets with EtherType **0x8138 (IPX)**.
`mac acl rule add 1 4 permit src any any dst any any`	To add a rule to position **4** of the MAC ACL with the ID **1** forwarding packets.
`show acl mac rules 1`	To display the rules of the MAC ACL with the ID **1**.
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	To change to the Interface Configuration mode of the interfaces **1/1** to **1/6**.

Command	Description
`acl mac assign 1 in 1`	To assign the MAC ACL with the ID **1** to incoming data packets (**1/1**) on interfaces **1/6** to **in**.
`exit`	To leave the interface mode.
`show acl mac assignment 1`	To display the assignment of the MAC ACL with the ID **1** to interfaces or VLANs.

Assigning ACLs to a Port or VLAN

When you assign ACLs to a port or VLAN, the device gives you the following options:

- To select the port or VLAN
- To specify the ACL priority
- To select the ACL using the group name

Perform the following steps:

Step	Action
1	Navigate to **Network Security > ACL > Assignment**.
2	Click the + button. The dialog displays the Create window: • In the **Port/VLAN** field, specify the desired port or the desired VLAN. • In the **Priority** field, specify the priority. • In the **Direction** field, specify the data packets to which the device applies the rule. • In the **Group name** field, specify the rule the device assigns to the port or the VLAN.
3	Click **OK**.
4	To apply the settings, click the ✓ button.

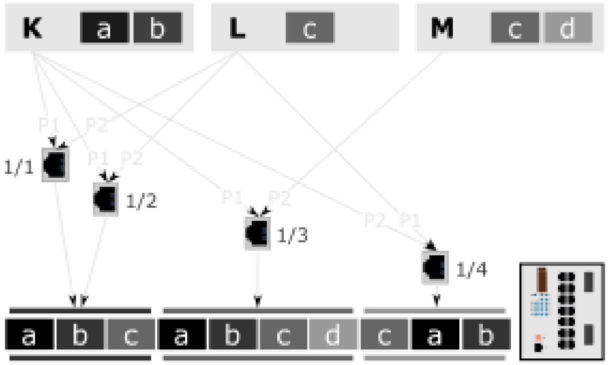
Maximum Number of Rules that Can be Assigned

The device allows a maximum of 50 ACLs, which can each contain a certain number of rules. The number of rules that you can actually assign to the ports and VLANs might be smaller than the number of rules specified in the device. The following example illustrates the factors that affect the possible number that you can actually assign.

In the device, 3 ACLs with a total of 4 rules are specified:

- ACL K containing the rules a and b
- ACL L containing the rule c
- ACL M containing the rules c and d

The ACLs and rules have symbolic names. Rules with the same name contain the same settings as presented in the following figure:



When assigning the ACLs to ports **1/1** to **1/4**, the device writes the rules contained in that ACLs with the specified priority to a hardware memory area that the ports and VLANs share. The order of the rules in relation to each other is determined by the index number within the respective ACL and by the assignment priority:

- Ports **1/1** and **1/2**

  Each port is assigned 3 identical rules. The order is the same because of the assignment priority.

  The device writes 3 rules to the hardware memory. Both ports share these rules.

- Port **1/3**

  The first 3 rules are identical to those for port **1/1**.

  The device writes the 3 rules again to the hardware memory, along with the additional fourth rule.

- Port **1/4**

  The rules are identical to those for port **1/1**.

  The device writes the 3 rules again to the hardware memory due to the changed order.

Port	Assigned ACLs	Applied rules	Number of rules	Occupied memory
1/1	K, L	a, b, c	3	3
1/2	K, L	a, b, c	0	3
1/3	K, M	a, b, c, d	4	7
1/4	L, K	c, a, b	3	10

Conclusion: Due to slight differences when assigning, four rules occupy the memory of ten rules. You can optimize the occupied memory by organizing the rules.

MAC Authentication Bypass

The MAC authorized bypass function allows clients that do not support 802.1X, such as printers and fax machines, authenticate to the network using their MAC address. The device allows specify the formatting of the MAC address used to authenticate the clients on the RADIUS server.

Example:

Split the MAC address into 6 groups of 2 characters. Use uppercase letters and a colon character as separator: **AA:BB:CC:DD:EE:FF**

Use the password **xY-45uM_e**. To do this, perform the following steps:

Step	Action
1	Navigate to **Network Security** > **802.1X** > **Global**. In the MAC authentication bypass format options frame, perform the following steps:
2	From the Group size drop-down list, select **2**. The device splits the MAC address into 6 groups of 2 characters.
3	From the Group separator drop-down list, select **:**.
4	From the uppercase or lowercase drop-down list, select **uppercase**.
5	In the **Password** field, enter the password **xY-45uM_e**. The device uses this password for every client that authenticates to the RADIUS server. If you leave the field empty, the device uses the formatted MAC address also as the password.
6	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dot1x mac-authentication-bypass format group-size 2`	To specify the group size **2**.
`dot1x mac-authentication-bypass format group-separator :`	To specify the group separator **:**.
`dot1x mac-authentication-bypass format letter-case upper-case`	To specify that the device formats the authentication data in uppercase letters.
`dot1x mac-authentication-bypass password xY-45uM_e`	To specify the password **xY-45uM_e**. The device uses this password to authenticate every client on the RADIUS server.

Network Load Control

The device features a number of functions that can help you reduce the network load:

- Direct packet distribution
- Multicasts
- Rate limiter
- Prioritization – QoS
- Flow control

Direct Packet Distribution

The device reduces the network load with direct packet distribution.

On each of its ports, the device learns the sender MAC address of received data packets. The device stores the combination of port and MAC address in its MAC address table (forwarding database).

By applying the *Store and Forward* method, the device buffers data received and verifies it for validity before forwarding it. The device rejects invalid and erroneous data packets.

Learning MAC Addresses

When the device receives a data packet, it verifies if the MAC address of the sender is already stored in the MAC address table (forwarding database). When the MAC address of the sender is undefined, the device generates an entry. The device then compares the destination MAC address of the data packet with the entries stored in the MAC address table (forwarding database):

- The device forwards packets with a defined destination MAC address directly to ports that have already received data packets from this MAC address.
- The device floods data packets with undefined destination addresses, that is, the device forwards these data packets to every port.

Aging of Learned MAC Addresses

Addresses that have not been detected by the device for an adjustable period of time (aging time) are deleted from the MAC address table (forwarding database) by the device. A reboot or resetting the MAC address table (forwarding database) deletes the entries in the MAC address table (forwarding database).

Static Address Entries

In addition to learning the sender MAC address, the device also provides the option to set MAC addresses manually. These MAC addresses remain configured and persist through resetting of the MAC address table (forwarding database) as well as rebooting of the device.

Static address entries allow the device to forward data packets directly to selected ports. If you do not specify a destination port, the device discards the corresponding data packets.

You can manage the static address entries in the Graphical User Interface or in the Command Line Interface by:

- Static Address Entries
- Converting a learned MAC address into a static address entry
- Disabling a static address entry
- Deleting learned MAC addresses

To create a static address entry, perform the following steps:

Step	Action
1	Navigate to **Switching** > **Filter for MAC Addresses**.
2	Add a user-configurable MAC address: • Click the + button. The dialog displays the Create window. • In the **MAC address** field, specify the destination MAC address. • In the **VLAN ID** field, specify the VLAN ID. • In the Port list, select the ports to which the device forwards data packets with the specified destination MAC address in the specified VLAN. When you have defined a unicast MAC address in the **MAC address** field, select only one port. When you have defined a multicast MAC address in the **MAC address** field, select one or more ports. If you want the device to discard data packets with the destination MAC address, do not select any port. • Click **OK**.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mac-filter <MAC address> <VLAN ID>`	To add the MAC address filter, consisting of a MAC address and VLAN ID.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`mac-filter <MAC address> <VLAN ID>`	To assign the port to a previously added MAC address filter.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

To convert a learned MAC address into a static address entry, perform the following steps:

Step	Action
1	Navigate to **Switching** > **Filter for MAC Addresses**.
2	To convert a learned MAC address into a static address entry, select the value **Permanent** in the Status column.
3	To apply the settings, click the ✓ button.

To disable a static address entry, perform the following steps:

Step	Action
1	Navigate to **Switching > Filter for MAC Addresses**.
2	To disable a static address entry, remove it from the table. To do this, select the table row that contains the value **Permanent** in the Status column, then click the ✕ button.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`no mac-filter <MAC address> <VLAN ID>`	To cancel the assignment of the MAC address filter on the port.
`exit`	To change to the Configuration mode.
`no mac-filter <MAC address> <VLAN ID>`	To delete the MAC address filter, consisting of a MAC address and a VLAN ID.
`exit`	To change to the Privileged EXEC mode.
`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

To delete learned MAC addresses, perform the following step:

Step	Action
1	To delete the learned addresses from the MAC address table (forwarding database), click the 🗑 button. As an alternative, Navigate to **Basic Settings > Restart** and click **Clear FDB**.

Execute the following command:

Command	Description
`clear mac-addr-table`	To delete the learned MAC addresses from the MAC address table (forwarding database).

Multicasts

By default, the device floods data packets with a multicast address, that is, the device forwards the data packets to every port. This leads to an increased network load.

The use of IGMP snooping can reduce the network load caused by multicast data packets. IGMP snooping lets the device send multicast data packets only on those ports to which devices using multicast are connected.

Example of a Multicast Application

Surveillance cameras transmit images to monitors in the machine room and in the monitoring room. With an IP multicast transmission, the cameras transmit their graphic data over the network in multicast packets.

The Internet Group Management Protocol (IGMP) organizes the data streams between the multicast routers and the monitors. The switches in the network between the multicast routers and the monitors monitor the IGMP data packets continuously (IGMP Snooping).

Switches register logins for receiving a multicast stream (IGMP report). The device then adds an entry in the MAC address table (forwarding database) and forwards multicast packets only to the ports on which it has previously received IGMP reports.

IGMP Snooping

The Internet Group Management Protocol (IGMP) describes the distribution of multicast information between routers and connected receivers on Layer 3. IGMP Snooping describes the function of a switch of continuously monitoring IGMP data packets and optimizing its own transmission settings for these data packets.

The IGMP Snooping function in the device operates according to RFC 4541 (*Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*).

Multicast routers with an active IGMP function periodically request (query) registration of multicast streams to determine the associated IP multicast group members. IP multicast group members reply with a Report message. This Report message contains the parameters required by the IGMP function. The multicast router enters the IP multicast group address from the Report message in its routing table. This causes it to forward data packets with this IP multicast group in the destination address field according to its routing table.

When leaving a multicast group (IGMP version 2 and greater), receivers log out with a “Leave” message and do not send any more Report messages. If it does not receive any more Report messages from this receiver within a certain time (aging time), the multicast router removes the routing table entry of a receiver.

When several IGMP multicast routers are in the same network, the device with the smaller IP address takes over the query function. When there are no multicast routers on the network, you have the option to enable the query function in an appropriately equipped switch.

A switch that connects one multicast receiver with a multicast router analyzes the IGMP information with the IGMP snooping method.

The IGMP snooping method also makes it possible for switches to use the IGMP function. A switch stores the MAC addresses derived from IP addresses of the multicast receivers as recognized multicast addresses in its MAC address table (forwarding database). In addition, the switch identifies the ports on which it has received reports for a specific multicast address. In this way, the switch forwards multicast packets only to ports to which multicast receivers are connected. The other ports do not receive these packets.

A special feature of the device is the possibility of determining the processing of data packets with undefined multicast addresses. Depending on the setting, the device discards these data packets or forwards them to every port. By default, the device transmits the data packets only to ports with connected devices, which in turn receive query packets. You also have the option of additionally sending defined multicast packets to query ports.

Setting IGMP Snooping

Perform the following steps:

Step	Action
1	Navigate to **Switching > IGMP Snooping > Global**.
2	Enable the IGMP Snooping function. Select the **On** radio button in the Operation frame. **NOTE:** When the IGMP Snooping function is disabled, the device behaves as follows: • The device ignores the received query and report messages. • The device forwards (floods) received data packets with a multicast address as the destination address to every port.
3	To apply the settings, click the ✓ button.

To specify the settings for a port, perform the following steps:

Step	Action
1	Navigate to the **Switching > IGMP Snooping > Configuration**, **Port** tab.
2	To activate the IGMP Snooping function on a port, select the checkbox in the Active column for the relevant port.
3	To apply the settings, click the ✓ button.

To specify the settings for a VLAN, perform the following:

Step	Action
1	Navigate to the **Switching > IGMP Snooping > Configuration**, **VLAN ID** tab.
2	To activate the IGMP Snooping function for a specific VLAN, select the checkbox in the Active column for the relevant VLAN.
3	To apply the settings, click the ✓ button.

Setting the IGMP Querier Function

The device itself optionally sends active query messages. As an alternative, the device responds to query messages or detects other multicast queriers in the network (Querier function).

Prerequisite:

The IGMP Snooping function is globally enabled.

Perform the following steps:

Step	Action
1	Navigate to **Switching > IGMP Snooping > Querier**.
2	In the Operation frame, enable/disable the Querier function of the device globally.
3	To activate the Querier function for a specific VLAN, select the checkbox in the Active column for the relevant VLAN. **Result:** The device carries out a selection process: When the IP source address of the other multicast querier is lower than its own, the device switches to the passive state, in which it does not send out any more query requests.
4	In the IP address column, you specify the IP multicast address that the device inserts as the sender address in generated query requests. You use the address of the multicast router.
5	To apply the settings, click the ✓ button.

IGMP Snooping Enhancements (Table)

The **Switching > IGMP Snooping > Snooping Enhancements** dialog provides you access to enhanced settings for the IGMP Snooping function. You activate or deactivate the settings on a per port basis in a VLAN.

The following settings are possible:

- **Static**

  Use this setting to set the port as a static query port. The device forwards every IGMP message on a static query port, even if it has previously received no IGMP query messages on this port. When the static option is disabled and the device has previously received IGMP query messages, it forwards IGMP messages on this port. When this is the case, the entry displays **L** (for learned).

- **Learn by LLDP**

  A port with this setting automatically discovers other Schneider Electric devices using the Link Layer Discovery Protocol (LLDP). The device then learns the IGMP query status of this port from these Schneider Electric devices and sets up the Querier function accordingly. The **ALA** entry indicates that the **Learn by LLDP** function is active. When the device has found another Schneider Electric device on this port in this VLAN, the entry also displays an **A** (for automatic).

- **Forward all**

  With this setting, the device forwards the data packets addressed to a multicast address to this port. The setting is suitable in the following situations, for example:

  - For diagnostic purposes.
  - For devices in an MRP Ring: After the ring is switched, the **Forward all** function makes it possible to reconfigure the network rapidly for data packets with registered multicast destination addresses. Activate the **Forward all** function on every ring port.

Prerequisite:

The IGMP Snooping function is globally enabled.

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **IGMP Snooping** > **Snooping Enhancements**.
2	Double-click the desired port in the desired VLAN.
3	To activate one or more functions, select the corresponding options.
4	Click **OK**.
5	To apply the settings, click the ✓ button.

Command	Description
`vlan database`	To change to the VLAN configuration mode.
`igmp-snooping vlan-id 1 forward-all 1/1`	To activate the **Forward All** function for port **1/1** in VLAN **1**.

Setting Up Multicasts

The device allows the exchange of multicast data packets. The device provides different options depending on whether the data packets are to be sent to undefined or defined multicast receivers.

The settings for undefined multicast addresses are global for the entire device. The following options can be selected:

- The device discards undefined multicasts.
- The device forwards undefined multicast data to every port.

NOTE: The exchange settings for undefined multicast addresses also apply to the reserved IP addresses from the *Local Network Control Block* (**224.0.0.0..224.0.0.255**). This behavior can affect greater-level routing protocols.

IGMP Snooping explicitly ignores the following multicast IP addresses because their mapped multicast MAC addresses have special functions:

Multicast IP address (es)	**Multicast MAC address(es)**	**Protocols (Block)**
224.0.0.0..224.0.0.255	01:00:5e:00:00:00..01:00:5e:00:00:ff	Local Network Control Block
224.0.1.1	01:00:5e:00:01:01	NTP/SNTP (Internetwork Control Block)
224.0.1.129..224.0.1.132	01:00:5e:00:01:81..01:00:5e:00:01:84	PTP (Internetwork Control Block)
239.255.16.12	01:00:5e:7f:10:0c	Ethernet Switch Configurator v2 (Administratively Scoped Block)

NOTE: According to RFC 1112 (*Host Extensions for IP Multicasting*), up to 32 multicast IP addresses are mapped to the same multicast MAC address. The table contains only the commonly used multicast IP address for a multicast MAC address, omitting the 31 further possible multicast IP addresses.

For each VLAN, you specify the sending of multicast packets to defined multicast addresses individually. The following options can be selected:

- The device forwards defined multicasts to the ports that have previously received query messages (query ports) and to the registered ports. Registered ports are ports with multicast receivers registered with the corresponding multicast group. This option helps ensure that the transfer works with basic applications without further configuration.
- The device forwards defined multicasts only to the registered ports. The advantage of this setting is that it uses the available bandwidth optimally through direct distribution.

Prerequisite:

The IGMP Snooping function is globally enabled.

Perform the following steps:

Step	**Action**
1	Navigate to **Switching** > **IGMP Snooping** > **Multicasts**.
2	In the Configuration frame, you specify how the device forwards data packets to undefined multicast addresses.
3	In the table, you specify how the device forwards data packets to defined multicast addresses. • **send to query and registered ports** The device forwards data packets with a defined MAC/IP multicast address to the query ports and to the registered ports. • **send to registered ports** The device forwards data packets with a defined MAC/IP multicast address to registered ports.
4	To apply the settings, click the ✓ button.

Rate Limiter

The rate limiter function helps ensure stable operation even with high data volumes by limiting the amount of data packets on the ports. The rate limitation is performed individually for each port, as well as separately for inbound and outbound data packets.

If the data rate on a port exceeds the defined limit, the device discards the overload on this port.

Rate limitation occurs entirely on Layer 2. In the process, the rate limiter function ignores protocol information on greater levels such as IP or TCP. This can affect the TCP data packets.

To minimize these effects, use the following options:

- Limit the rate limitation to certain packet types, for example, broadcasts, multicasts, and unicasts with an undefined destination address.
- Limit the amount of outbound data packets instead of the inbound data packets. The outbound rate limitation works better with TCP flow control due to device-internal buffering of the data packets.
- Increase the aging time for learned unicast addresses.

Perform the following steps:

Step	Action
1	Navigate to **Switching > Rate Limiter**.
2	Activate the rate limiter and set limits for the data rate. The settings apply on a per port basis and are separated according to the type of the data packets: • Received broadcast data packets • Received multicast data packets • Received unicast data packets with an undefined destination address To activate the rate limiter on a port, select the checkbox for at least one category. In the Unit column, you specify if the device interprets the threshold values as percent of the port bandwidth or as packets per second. The threshold value **0** deactivates the rate limiter.
3	To apply the settings, click the ✓ button.

QoS/Priority

QoS (Quality of Service) is a procedure defined in IEEE 802.1D which is used to distribute resources in the network. QoS allows the prioritization the data of necessary applications.

When there is a heavy network load, prioritizing helps prevent data packets with lower priority from interfering with delay-sensitive data packets. Delay-sensitive data packets include, for example, voice, video, and real-time data.

Description of Prioritization

For data packet prioritization, *traffic classes* are defined in the device. The device prioritizes greater *traffic classes* over lower *traffic classes*. The number of *traffic classes* depends on the device type.

To provide for optimal data flow for delay-sensitive data, you assign greater *traffic classes* to this data. You assign lower *traffic classes* to data that is less sensitive to delay.

Assigning *traffic classes* to the Data

The device automatically assigns *traffic classes* to inbound data (traffic classification). The device takes the following classification criteria into account:

- Methods according to which the device carries out assignment of received data packets to *traffic classes*:
  - **trustDot1p**

    The device uses the priority of the data packet contained in the VLAN tag.
  - **trustIpDscp**

    The device uses the QoS information contained in the IP header (ToS/DiffServ).
  - **untrusted**

    The device ignores possible priority information within the data packets and uses the priority of the receiving port directly.
- The priority assigned to the receiving port.

Both classification criteria are configurable.

During traffic classification, the device uses the following rules:

- When the receiving port is set to **trustDot1p** (default setting), the device uses the data packet priority contained in the VLAN tag. When the data packets do not contain a VLAN tag, the device is guided by the priority of the receiving port.
- When the receiving port is set to **trustIpDscp**, the device uses the QoS information (ToS/DiffServ) in the IP header. When the data packets do not contain IP packets, the device is guided by the priority of the receiving port.
- When the receiving port is set to **untrusted**, the device is guided by the priority of the receiving port.

Prioritizing *traffic classes*

For prioritization of *traffic classes*, the device uses the following methods:

- *Strict Priority*

  When transmission of data of a greater *traffic class* is no longer taking place or the relevant data is still in the queue, the device sends data of the corresponding *traffic class*. If every *traffic class* is prioritized according to the *Strict Priority* method, under high network load the device can permanently block the data of lower *traffic classes*.
- *Weighted Fair Queuing*

  The *traffic class* is assigned a specific bandwidth. This helps ensure that the device sends the data packets of this *traffic class*, although there is a lot of data packets in greater *traffic classes*.

Handling of Received Priority Information

Applications label data packets with the following prioritization information:

- VLAN priority according to IEEE 802.1Q (Layer 2)
- Type-of-Service (ToS) or DiffServ (DSCP) for VLAN Management IP packets (Layer 3)

The device allows priority information using the following options:

- **trustDot1p**

  The device assigns VLAN-tagged data packets to the different *traffic classes* according to their VLAN priorities. The corresponding allocation is configurable. The device assigns the priority of the receiving port to data packets it receives without a VLAN tag.
- **trustIpDscp**

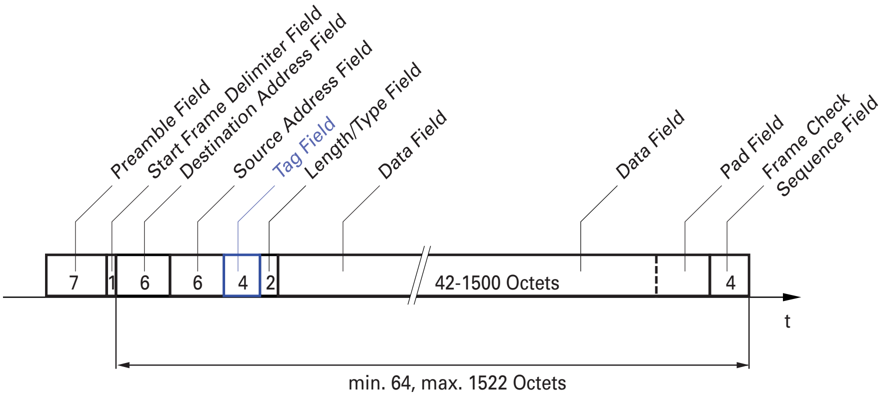
  The device assigns the IP packets to the different *traffic classes* according to the DSCP value in the IP header, although the packet was also VLAN-tagged. The corresponding allocation is configurable. The device prioritizes non-IP packets according to the priority of the receiving port.
- **untrusted**

  The device ignores the priority information in the data packets and assigns the priority of the receiving port to them.

VLAN Tagging

For the VLAN and prioritizing functions, IEEE 802.1Q provides for integrating a MAC frame in the VLAN tag. The VLAN tag consists of four bytes and is between the source address field (“Source Address Field”) and type field (“Length / Type Field”).

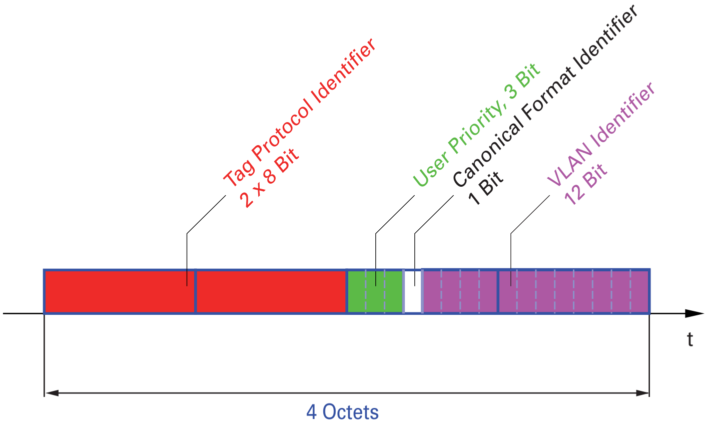
The following figure presents ethernet data packet with the VLAN tag:



For data packet with VLAN tags, the device evaluates the following information:

- Priority information
- When VLANs are set up, VLAN tagging

The following figure presents the structure of the VLAN tagging



A data packet with VLAN tag containing priority information but no VLAN information (VLAN ID = 0), is a *Priority Tagged* frame.

NOTE: Network protocols and redundancy mechanisms use the highest *traffic class* 7. Therefore, select other *traffic classes* for application data.

When using VLAN prioritizing, consider the following special features:

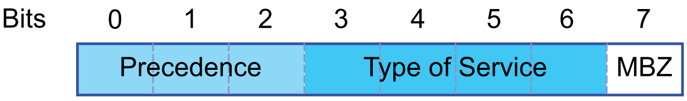
- End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network. The prerequisite is that every network component is VLAN-capable.
- Routers are not able to send and receive packets with VLAN tags through port-based router interfaces.

IP ToS (Type of Service)

The Type-of-Service field (ToS) in the IP header was already part of the IP protocol from the start, and is used to differentiate different services in IP networks. Even back then, there were ideas about differentiated treatment of IP packets, due to the limited bandwidth available and the unreliable connection paths. Because of the continuous increase in the available bandwidth, there was no need to use the ToS field.

Only with the real-time requirements of today's networks has the ToS field become significant again. Selecting the ToS byte of the IP header allows differentiation between different services. However, this field is not widely used in practice.

The following figure presents the ToS field:



The following table describes the ToS field in the IP header:

Bits (0-2): IP Precedence Defined	**Bits (3-6): Type of Service Defined**	**Bit (7)**
111 - Network Control	0000 - [all normal]	0 - Zero
110 - Internetwork Control	1000 - [minimize delay]	–
101 - CRITIC / ECP	0100 - [maximize throughput	–
100 - Flash Override	0010 - [maximize reliability]	–
011 - Flash	0001 - [minimize monetary cost]	–
010 - Immediate	–	–
001 - Priority	–	–
000 - Routine	–	–

Handling of *traffic classes*

The device provides the following options for handling *traffic classes*:

- *Strict Priority*
- *Weighted Fair Queuing*
- *Strict Priority* combined with *Weighted Fair Queuing*
- Queue management

Strict Priority Description

With the *Strict Priority* setting, the device first transmits data packets that have a greater *traffic class* (greater priority) before transmitting a data packet with the next highest *traffic class*. When there are no other data packets remaining in the queue, the device transmits a data packet with the lowest *traffic class* (lowest priority). In some cases, if there is a high volume of high-priority data packets waiting to be sent on this port, the device does not send data packets with a low priority.

In delay-sensitive applications, such as VoIP or video, *Strict Priority* allows data to be sent immediately.

Weighted Fair Queuing Description

With *Weighted Fair Queuing*, also called *Weighted Round Robin (WRR)*, you assign a minimum or reserved bandwidth to each *traffic class*. This helps ensure that data packets with a lower priority are also sent although the network is very busy.

The reserved values range from 0% through 100% of the available bandwidth, in steps of 1%.

- A reservation of 0 is equivalent to a "no bandwidth" setting.
- The sum of the individual bandwidths can be up to 100%.

When you assign *Weighted Fair Queuing* to every *traffic class*, the entire bandwidth of the corresponding port is available to you.

Combining *Strict Priority* and *Weighted Fair Queuing*

When combining *Weighted Fair Queuing* with *Strict Priority*, verify that the highest *traffic class* of *Weighted Fair Queuing* is lower than the lowest *traffic class* of *Strict Priority*.

If you combine *Weighted Fair Queuing* with *Strict Priority*, a high *Strict Priority* network load can significantly reduce the bandwidth available for *Weighted Fair Queuing*.

Queue Management

Queue Shaping

Queue Shaping throttles the rate at which queues transmit packets. For example, using Queue Shaping, you rate-limit a greater strict-priority queue so that it allows a lower strict-priority queue to send packets even though greater priority packets are still available for transmission. The device allows Queue Shaping for any queue. You specify Queue Shaping as the maximum rate at which the data packets pass through a queue by assigning a percentage of the available bandwidth.

Defining Settings for Queue Management

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **QoS/Priority** > **Queue Management**.
2	The total assigned bandwidth in the Min. bandwidth [%] column is 100%.
3	To activate *Weighted Fair Queuing* for Traffic class = **0**, proceed as follows: • Clear the checkbox in the Strict priority column. • In the Min. bandwidth [%] column, specify the value **5**.
4	To activate *Weighted Fair Queuing* for Traffic class = **1**, proceed as follows: • Clear the checkbox in the Strict priority column. • In the Min. bandwidth [%] column, specify the value **20**.
5	To activate *Weighted Fair Queuing* for Traffic class = **2**, proceed as follows: • Clear the checkbox in the Strict priority column. • In the Min. bandwidth [%] column, specify the value **30**.
6	To activate *Weighted Fair Queuing* for Traffic class = **3**, proceed as follows: • Clear the checkbox in the Strict priority column. • In the Min. bandwidth [%] column, specify the value **20**.
7	To activate *Weighted Fair Queuing* and Queue Shaping for Traffic class = **4**, proceed as follows: • Clear the checkbox in the Strict priority column. • In the Min. bandwidth [%] column, specify the value **10**. • In the Max. bandwidth [%] column, specify the value **10**. When using a *Weighted Fair Queuing* and Queue Shaping combination for a specific *traffic class*, specify a greater value in the Max. bandwidth [%] column than the value specified in the Min. bandwidth [%] column.
8	To activate *Weighted Fair Queuing* for Traffic class = **5**, proceed as follows: • Clear the checkbox in the Strict priority column. • In the Min. bandwidth [%] column, specify the value **5**.
9	To activate *Weighted Fair Queuing* for Traffic class = **6**, proceed as follows: • Clear the checkbox in the Strict priority column. • In the Min. bandwidth [%] column, specify the value **10**.
10	To activate *Strict Priority* and Queue Shaping for Traffic class = **7**, proceed as follows: • Select the checkbox in the Strict priority column. • In the Max. bandwidth [%] column, specify the value **10**.
11	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`cos-queue weighted 0`	To enable *Weighted Fair Queuing* for *traffic class* **0**.
`cos-queue min-bandwidth: 0 5`	To assign a weight of **5** % to *traffic class* **0**.
`cos-queue weighted 1`	To enable *Weighted Fair Queuing* for *traffic class* **1**.
`cos-queue min-bandwidth: 1 20`	To assign a weight of **20** % to *traffic class* **1**.
`cos-queue weighted 2`	To enable *Weighted Fair Queuing* for *traffic class* **2**.
`cos-queue min-bandwidth: 2 30`	To assign a weight of **30** % to *traffic class* **2**.
`cos-queue weighted 3`	To enable *Weighted Fair Queuing* for *traffic class* **3**.
`cos-queue min-bandwidth: 3 20`	To assign a weight of **20** % to *traffic class* **3**.

```
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         0               0               strict
5         0               0               strict
6         0               0               strict
7         0               0               strict
```

Combining *Weighted Fair Queuing* and Queue Shaping

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`cos-queue weighted 4`	To enable *Weighted Fair Queuing* for *traffic class* **4**.
`cos-queue min-bandwidth: 4 10`	To assign a weight of **10** % to *traffic class* **4**.
`cos-queue max-bandwidth: 4 10`	To assign a weight of **10** % to *traffic class* **4**.
`cos-queue weighted 5`	To enable *Weighted Fair Queuing* for *traffic class* **5**.
`cos-queue min-bandwidth: 5 5`	To assign a weight of **5** % to *traffic class* **5**.
`cos-queue weighted 6`	To enable *Weighted Fair Queuing* for *traffic class* **6**.
`cos-queue min-bandwidth: 6 10`	To assign a weight of **10** % to *traffic class* **6**.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               0               strict
```

Setting Up Queue Shaping

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`cos-queue max-bandwidth: 7 10`	To assign a weight of **10** % to *traffic class* **7**.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               10              strict
```

Management Prioritization

The device allows management packets so that you can access the device management at any time in situations with high network load.

When prioritizing management packets, the device sends the management packets with priority information.

- On Layer 2, the device modifies the VLAN priority in the VLAN tag.

  The prerequisite for this function is that the corresponding ports are set to allow sending packets with a VLAN tag.
- On Layer 3, the device modifies the IP-DSCP value.

Setting Prioritization

Assigning the *Port priority*

Perform the following steps:

Step	Action
1	Navigate to **Switching > QoS/Priority > Port Configuration**.
2	In the Port priority column, you specify the priority with which the device forwards the data packets received on this port without a VLAN tag.
3	In the Trust mode column, you specify the criteria the device uses to assign a *traffic class* to data packets received.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`vlan priority 3`	To assign interface **1/1** the *Port priority* **3**.
`exit`	To change to the Configuration mode.

Assigning VLAN Priority to a *traffic class*

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **QoS/Priority** > **802.1D/p Mapping**.
2	To assign a *traffic class* to a VLAN priority, insert the associated value in the Traffic class column.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`classofservice dot1p-mapping 0 2`	To assign a VLAN priority of **0** to *traffic class* **2**.
`classofservice dot1p-mapping 1 2`	To assign a VLAN priority of **1** to *traffic class* **2**.
`exit`	To change to the Privileged EXEC mode.
`show classofservice dot1p-mapping`	To display the assignment.

Assigning *Port priority* to Received Data Packets

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`classofservice trust untrusted`	To assign the **untrusted** mode to the interface.

`classofservice dot1p-mapping 0 2`
`classofservice dot1p-mapping 1 2`
	To assign a VLAN priority of **0** to *traffic class* **2**.
	To assign a VLAN priority of **1** to *traffic class* **2**.

`vlan priority 1`	To specify the value **1** for the *Port priority*.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.
`show classofservice trust`	To display the Trust mode of the ports/interfaces.

```
 Interface Trust Mode
 --------- -------------
 1/1       untrusted
 1/2       dot1p
 1/3       dot1p
 1/4       dot1p
 1/5       dot1p
 1/6       dot1p
 1/7       dot1p
```

Assigning DSCP to a *traffic class*

Perform the following steps:

Step	Action
1	Navigate to **Switching > QoS/Priority > IP DSCP Mapping**.
2	Specify the desired value in the Traffic class column.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`classofservice ip-dscp-mapping cs1 1`	To assign the DSCP value **CS1** to *traffic class* **1**.
`show classofservice ip-dscp-mapping`	To display the IP DSCP assignments

```
    IP DSCP       Traffic Class
 -------------    -------------
   be                  2
   1                   2
   .                   .
   .                   .
   (cs1)               1
   .                   .
```

Assigning the DSCP Priority to Received IP Data Packets

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`classofservice trust ip-dscp`	To assign the **trust ip-dscp** mode globally.
`exit`	To change to the Configuration mode.
`show classofservice trust`	To display the Trust mode of the ports/interfaces.

```
Interface     Trust Mode
----------    -------------
1/1           ip-dscp
1/2           dot1p
1/3           dot1p
.             .
.             .
1/5           dot1p
.             .
```

Configuring Traffic Shaping on a Port

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface **1/2**.
`traffic-shape bw 50`	To limit the maximum bandwidth of the port **1/2** to 50%.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.
`show traffic-shape`	To display the Traffic Shaping configuration.

```
Interface  Shaping rate
---------  ------------
1/1        0  %
1/2        50 %
1/3        0  %
1/4        0  %
```

Configuring Layer 2 Management Priority

Perform the following steps:

Step	Action
1	Navigate to **Switching > QoS/Priority > Global**.
2	In the VLAN priority for management packets field, specify the VLAN priority with which the device sends management data packets.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`network management priority dot1p 7`	To assign the VLAN priority of **7** to management packets. The device sends management packets with the highest priority.
`show network parms`	To display the priority of the VLAN in which the device management is located.

```
IPv4 Network
------------
...
Management VLAN priority...................7
...
```

Configuring Layer 3 Management Priority

Perform the following steps:

Step	Action
1	• Navigate to **Switching > QoS/Priority > Global**.
2	• In the IP DSCP value for management packets field, specify the DSCP value with which the device sends management data packets.
3	• To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`network management priority ip-dscp 56`	To assign the DSCP value of **56** to management packets. The device sends management packets with the highest priority.
`show network parms`	To display the priority of the VLAN in which the device management is located.

```
IPv4 Network
------------
...
Management IP-DSCP value...................56
```

Flow Control

If a large number of data packets are received in the priority queue of a port at the same time, this can cause the port memory to overflow. This happens, for example, when the device receives data on a Gigabit port and forwards it to a port with a lower bandwidth. The device discards superfluous data packets.

The flow control mechanism defined in IEEE 802.3 helps ensure that no data packets are lost due to buffer overflow on a port. Shortly before the buffer memory of a port is completely full, the device signals to the connected devices that it is not accepting any more data packets from them:

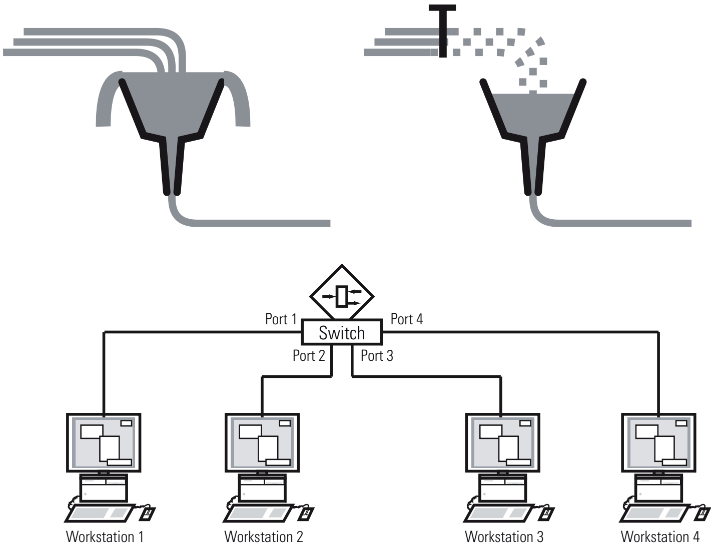
- In full-duplex mode, the device sends a pause data packet.
- In half-duplex mode, the device simulates a collision.

The following figure displays how flow control works. Workstations 1, 2, and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2, and 3 is greater than the bandwidth of

Workstation 4. This causes an overflow on the receive queue of port 4. The left funnel symbolizes this status.

When the flow control function on ports 1, 2 and 3 of the device is enabled, the device reacts before the funnel overflows. The funnel on the right illustrates ports 1, 2 and 3 sending a message to the transmitting devices to control the rate of transmission. This results in the receiving port no longer being overwhelmed and can process the incoming data packets.

The following figure presents an example of flow control:



Flow Control with a Half-Duplex Link

In the example presented in Flow Control, page 156, there is a half-duplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends data back to Workstation 2. Workstation 2 detects a collision and stops transmitting.

Flow Control with a Full-Duplex Link

In the example presented in Flow Control, page 156 , there is a full-duplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends a request to Workstation 2 to include a short delay in the sending transmission.

Setting Up the Flow Control

Perform the following steps:

Step	Action
1	Navigate to **Switching > Global**.
2	Select the Flow control checkbox. With this setting you enable flow control in the device.
3	Navigate to the **Basic Settings > Port**, **Configuration** tab.

Step	Action
4	To enable the Flow Control on a port, select the checkbox in the Flow control column.
5	To apply the settings, click the ✓ button.

NOTE: When you are using a redundancy function, you deactivate the flow control on the participating ports. If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.

Configuring Template-Based TSN

Underlying Facts

When you use the TSN function, the following basic conditions apply:

- The device operates using the *Store and Forward* method. Thus, the device has to receive the complete data packet before it makes a forwarding decision.
- You specify the Base time and Cycle time once in the device. Both settings are valid for each port participating in TSN.
- You set up a Gate Control List per port based on predefined templates for easier setup.
- Verify that the sum of the Gate Control List entry times is less than or equal to the specified Cycle time.
- The device uses a guard band to help protect the time slot for high priority packets from packets that "leak" from the previous time slot. The decisive factor for the interval length of the guard band is the port speed of the sending port.

  Use the following interval lengths for the guard band. The values are based on the port speed and the maximum allowed size of Ethernet packets:

  - 2.5 Gbit/s: 5 µs
  - 1 Gbit/s: 13 µs
  - 100 Mbit/s: 124 µs
- The Cycle time range is 50,000..10,000,000 ns.
- The Gate Control List interval range is 1,000..10,000,000 ns.
- Verify that the Cycle time as well as the Gate Control List intervals are multiples of 1 µs, 2 µs or 4 µs.

The following table presents dependency between Cycle time and granularity:

Cycle time	**Granularity**
50 µs..4 ms	1 µs
4.002 ms..8 ms	2 µs
8.004 ms..10 ms	4 µs

Application Example for Template-Based TSN

This example describes how to set up the devices for a scenario with the following conditions:

- Cycle time = 1 ms
- Time slot for high priority packets = 500 µs
- Time slot for low-priority packets = 487 µs

In this example, each device is connected to the network with a port speed of 1 Gbit/s.

The following table presents the cycle structure:

Time slot	***Traffic classes***	**Duration**
High priority packets	7	500 µs
Low-priority packets	0,1,2,3,4,5,6	487 µs
Guard band	–	13 µs

Time Calculation

The device automatically calculates the duration of the time slot for low-priority packets. The calculation is based on the following parameters:

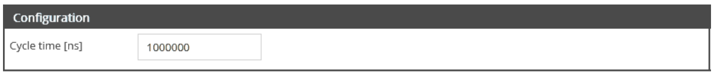
- Cycle time
- Duration of the time slot for high priority packets
- Duration of the guard band

Setting Up the Devices

Using the previously specified times, you set up the devices using the Graphical User Interface or the Command Line Interface. For each device involved, perform the following steps.

Checking and Adjusting the Cycle Time

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **TSN** > **Configuration**.
2	In the Configuration frame, verify the value in the **Cycle time [ns]** field.
3	If necessary, adjust the value:  Configuration Cycle time [ns] 1000000
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.

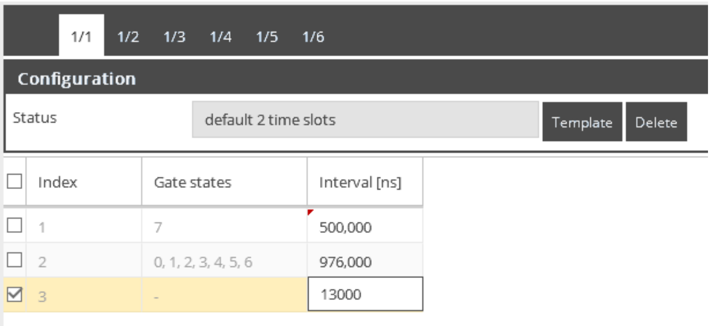
```
show tsn configuration
Port  Status                 Conf. cycle time[ns]  Conf. base time
      Default gate states    Curr. cycle time[ns]  Curr. base time
      Config change pending                        Time of last
activation
----  ---------------------  --------------------
-----------------------------
 1/1  [x]           disabled              1000000  1970-01-01
00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01
00:00:00.000000000
      [ ]                                          2018-07-12
08:10:58.813000000
 1/2  [x]           disabled              1000000  1970-01-01
00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01
00:00:00.000000000
      [ ]                                          2018-07-11
07:24:35.204000000
 1/3  [ ]          disabled               1000000  1970-01-01
00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01
00:00:00.000000000
      [ ]                                          1970-01-01
00:00:00.000000000
 1/4  [ ]          disabled               1000000  1970-01-01
00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01
00:00:00.000000000
      [ ]                                          1970-01-01
00:00:00.000000000
```

Command	Description
`tsn cycle-time 1000000`	If necessary, adjust the value.

Selecting a Template and Setting Up the Gate Control List

The device provides predefined templates to help you set up the Gate Control List. The following example guides you through the necessary steps using the template **default 2 time slots**. After you select the template, you can adjust the duration of the time slots. Perform the following steps for each port for which you want to use the TSN function.

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **TSN** > **Gate Control List** > **Configured**.
2	Select the tab for the port for which you want to specify the settings.
3	Select a template in the Configuration frame. Perform the following steps: • Click **Template**. • Select **default 2 time slots**. • Click **OK**.
4	Adjust the values in the Interval [ns] column: • Enter the value **500000** in the row for high priority packets. • Enter the value **13000** in the row for the guard band. • The device calculates the third value automatically when saving the changes.  1/1 1/2 1/3 1/4 1/5 1/6 Configuration Status: default 2 time slots [Template] [Delete] □ Index | Gate states | Interval [ns] □ 1 | 7 | 500,000 □ 2 | 0, 1, 2, 3, 4, 5, 6 | 976,000 ☑ 3 | - | 13000
5	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`tsn gcl modify 1 interval 500000`	To adjust the duration in nanoseconds of the time slot for high priority packets.
`tsn gcl modify 3 interval 13000`	To adjust the duration in nanoseconds of the time slot for the guard band. The device automatically calculates the duration of the time slot for low-priority packets. You cannot set the time slot for low-priority packets.

VLANs

In the simplest case, a virtual LAN (VLAN) consists of a group of network participants in one network segment who can communicate with each other as though they belonged to a separate LAN.

More complex VLANs span out over multiple network segments and are also based on logical (instead of only physical) connections between network participants. VLANs are elements of flexible network design. It is easier to reconfigure logical connections centrally than cable connections.

The device supports independent VLAN learning according to IEEE 802.1Q which defines the VLAN function.

Using VLANs has many benefits. The following list displays the top benefits:

- Network load limiting

  VLANs reduce the network load considerably as the devices transmit broadcast, multicast, and unicast packets with undefined (unlearned) destination addresses only inside the virtual LAN. The rest of the data network forwards the data packets as normal.
- Flexibility

  You have the option of forming user groups based on the function of the participants apart from their physical location or medium.
- Clarity

  VLANs give networks a clear structure and make maintenance easier.

Examples of VLANs

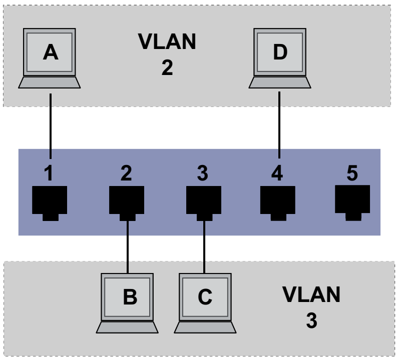
The following practical examples provide an introduction to the structure of a VLAN.

NOTE: When configuring VLANs you use an interface for accessing device management that will remain unchanged. For this example, you use either interface 1/6 or the serial connection to set up the VLANs.

Application Example of a Port-Based VLAN

The example displays a minimal VLAN configuration (port-based VLAN). An administrator has connected multiple end devices to a transmission device and assigned them to 2 VLANs. This effectively prohibits any data transmission between the VLANs, whose members communicate only within their own VLANs.

The following figure presents an example of a port-based VLAN:



When setting up the VLANs, you add communication rules for every port, which you set up in ingress (incoming) and egress (outgoing) tables.

The ingress table specifies which VLAN ID a port assigns to the incoming data packets. Hereby, you use the port address of the end device to assign it to a VLAN:

Terminal	Port	Port VLAN identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
–	5	1

The egress table specifies on which ports the device sends the packets from this VLAN:

- **T** = Tagged (with a tag field, selected)
- **U** = Untagged (without a tag field, cleared)

For this example, the status of the TAG field of the data packets has no relevance, so you use the setting **U**:

VLAN ID	Port				
	1	**2**	**3**	**4**	**5**
1	–	–	–	–	U
2	U	–	–	U	–
3	–	U	U	–	–

To set up the VLAN, perform the following steps:

Step	Action
1	Navigate to **Switching > VLAN > Configuration**.
2	Click the ⊞ button. The dialog displays the Create window.
3	In the **VLAN ID** field, specify the value **2**.
4	Click **OK**.
5	For the VLAN, specify the name **VLAN2**: Double-click the **Name** column and specify the name. For VLAN **1**, in the **Name** column, change the value **Default** to **VLAN1**.
6	Repeat the previous steps to add VLAN **3** with the name **VLAN3**.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 2`	To add VLAN **2**.
`name 2 VLAN2`	To assign the name **2** to the VLAN **VLAN2**.
`vlan add 3`	To add VLAN **3**.
`name 3 VLAN3`	To assign the name **3** to the VLAN **VLAN3**.
`name 1 VLAN1`	To assign the name **1** to the VLAN **VLAN1**.
`exit`	To change to the Privileged EXEC mode.
`show vlan brief`	To display the present VLAN configuration.

```
Max. VLAN ID................................. 4042
Max. supported VLANs......................... 128
Number of currently configured VLANs......... 3
vlan unaware mode............................ disabled
VLAN ID VLAN Name                      VLAN Type VLAN Creation Time
---- ------------------------------    --------- ------------------
1      VLAN1                           default    0 days, 00:00:05
2      VLAN2                           static     0 days, 02:44:29
3      VLAN3                           static     0 days, 02:52:26
```

To set up the ports, perform the following steps:

Step	Action
1	Navigate to **Switching** > **VLAN** > **Configuration**.
2	To assign the port to a VLAN, specify the desired value in the corresponding column. Possible values: • **T** The port is a member of the VLAN. The port transmits tagged data packets. • **U** The port is a member of the VLAN. The port transmits untagged data packets. • **F** The port is not a member of the VLAN. Changes using the GVRP function are disabled. • **-** The port is not a member of the VLAN. Changes using the GVRP function are allowed. Because end devices usually interpret untagged data packets, you specify the value **U**.
3	To apply the settings, click the ✓ button.
4	Navigate to **Switching** > **VLAN** > **Port**. The prerequisite is that the port does not operate in a private VLAN.
5	In the Port-VLAN ID column, specify the related VLAN: **2** or **3**
6	Because end devices usually interpret untagged data packets, in the Acceptable packet types column, you specify the value **admitAll** for ports connected to an end device.
7	To apply the settings, click the ✓ button.
8	The value in the Ingress filtering column has no affect on how this example functions.

Execute the following commands:

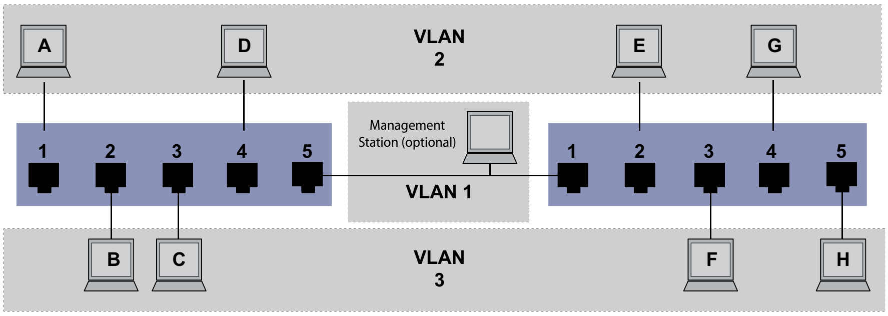
Command	**Description**
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`vlan participation include 2`	The port **1/1** becomes a member of the VLAN **2** and transmits the data packets without a VLAN tag.
`vlan pvid 2`	To assign the Port VLAN ID **1/1** to port **2**.
`exit`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface **1/2**.
`vlan participation include 3`	The port **1/2** becomes a member of the VLAN **3** and transmits the data packets without a VLAN tag.
`vlan pvid 3`	To assign the Port VLAN ID **1/2** to port **3**.
`exit`	To change to the Configuration mode.
`interface 1/3`	To change to the Interface Configuration mode of interface **1/3**.
`vlan participation include 3`	The port **1/3** becomes a member of the VLAN **3** and transmits the data packets without a VLAN tag.
`vlan pvid 3`	To assign the Port VLAN ID **1/3** to port **3**.
`exit`	To change to the Configuration mode.
`interface 1/4`	To change to the Interface Configuration mode of interface **1/4**.
`vlan participation include 2`	The port **1/4** becomes a member of the VLAN **2** and transmits the data packets without a VLAN tag.
`vlan pvid 2`	To assign the Port VLAN ID **1/4** to port **2**.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.

Command	Description
`show vlan id 3`	To display details for VLAN **3**.

```
VLAN ID          : 3
VLAN Name        : VLAN3
VLAN Type        : Static
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1            -      Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4            -      Autodetect   Tagged
1/5            -      Autodetect   Tagged
```

Application Example of a Complex VLAN Setup

This example presents a complex configuration with 3 VLANs (1 to 3). Along with the switch from the previous example of a simple port-based VLAN, page 163, you use a second switch (on the right in the following figure):



The terminal devices (A to H) of the individual VLANs are spread over 2 transmission devices (Switches). Such VLANs are defined as distributed VLANs. An optional network PC is also shown, which has access to the device management of each network component if the associated VLAN is set up correctly.

> **NOTE:** In this case, VLAN 1 has no significance for the end device communication, but it is required for the administration of the transmission devices through the Management VLAN.

As in the previous example, uniquely assign the ports with their connected terminal devices to a VLAN. With the direct connection between both transmission devices (uplink), the ports transport packets for both VLANs. To differentiate these uplinks you use “VLAN tagging”, which handles the data packets accordingly. Thus, you maintain the assignment to the respective VLANs.

Perform the following steps:

- Add Uplink Port 5 to the ingress and egress tables from the previous example of a simple port-based VLAN, page 163.
- Create new ingress and egress tables for the right switch, as described in the previous example of a simple port-based VLAN, page 163.

The egress table specifies on which ports the device sends the packets from this VLAN:

- **T** = Tagged (with a tag field, selected)
- **U** = Untagged (without a tag field, cleared)

In this example, tagged packets are used in the communication between the transmission devices (Uplink), as packets for different VLANs are differentiated at these ports.

The following table is an ingress table for devices on the left:

Terminal	Port	Port VLAN identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

The following table is an ingress table for devices on the right:

Terminal	Port	Port VLAN identifier (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

The following table is an egress table for devices on the left:

VLAN ID	Port				
	1	2	3	4	5
1	–	–	–	–	U
2	U	–	–	U	T
3	–	U	U	–	T

The following table is an egress table for devices on the right:

	Port				
VLAN ID	1	2	3	4	5
1	U	–	–	–	–
2	T	U	–	U	–
3	T	–	U	–	U

The communication relationships here are as follows: end devices on ports 1 and 4 of the left device and end devices on ports 2 and 4 of the right device are members of VLAN 2 and can thus communicate with each other. The behavior is the same for the end devices on ports 2 and 3 of the left device and the end devices on ports 3 and 5 of the right device. These belong to VLAN 3.

The end devices “see” their respective part of the network. Participants outside this VLAN cannot be reached. The device also sends broadcast, multicast, and unicast packets with undefined (unlearned) destination addresses only inside a VLAN.

Here, the devices use VLAN tagging (IEEE 801.1Q) within the VLAN with the ID 1 (Uplink). The letter **T** in the egress table of the ports indicates VLAN tagging.

The configuration of the example is the same for the device on the right. Proceed in the same way, using the ingress and egress tables previously specified to adapt the previously set up left device to the new environment.

To set up the VLAN, perform the following steps:

Step	Action
1	Navigate to **Switching** > **VLAN** > **Configuration**.
2	Click the + button. The dialog displays the Create window.
3	In the **VLAN ID** field, specify the VLAN, for example **2**.
4	Click **OK**.
5	For the VLAN, specify the name **VLAN2**: Double-click the **Name** column and specify the name. For VLAN **1**, in the **Name** column, change the value **Default** to **VLAN1**.
6	Repeat the previous steps to add VLAN **3** with the name **VLAN3**.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 2`	To add VLAN **2**.
`name 2 VLAN2`	To assign the name **2** to the VLAN **VLAN2**.
`vlan add 3`	To add VLAN **3**.
`name 3 VLAN3`	To assign the name **3** to the VLAN **VLAN3**.
`name 1 VLAN1`	To assign the name **1** to the VLAN **VLAN1**.
`exit`	To change to the Privileged EXEC mode.
`show vlan brief`	To display the present VLAN configuration.

```
Max. VLAN ID................................ 4042
Max. supported VLANs........................ 128
Number of currently configured VLANs........... 3
vlan unaware mode............................ disabled
VLAN ID VLAN Name                      VLAN Type VLAN Creation Time
---- ------------------------------ --------- ------------------
1      VLAN1                           default    0 days, 00:00:05
2      VLAN2                           static     0 days, 02:44:29
3      VLAN3                           static     0 days, 02:52:26
```

To set up the ports, perform the following steps:

Step	Action
1	Navigate to **Switching > VLAN > Configuration**.
2	To assign the port to a VLAN, specify the desired value in the corresponding column. Possible values: • **T** The port is a member of the VLAN. The port transmits tagged data packets. • **U** The port is a member of the VLAN. The port transmits untagged data packets. • **F** The port is not a member of the VLAN. Changes using the GVRP function are disabled. • **-** The port is not a member of the VLAN. Changes using the GVRP function are disabled. Because end devices usually interpret untagged data packets, you specify the value **U**. You specify the **T** setting on the uplink port on which the VLANs communicate with each other.
3	To apply the settings, click the ✓ button.
4	Navigate to **Switching > VLAN > Port**. The prerequisite is that the port does not operate in a private VLAN.
5	In the Port-VLAN ID column, specify the related VLAN: **1**, **2** or **3**
6	Because end devices usually interpret untagged data packets, in the Acceptable packet types column, you specify the value **admitAll** for ports connected to an end device.
7	For the uplink port, in the Acceptable packet types column, specify the value **admitOnlyVlanTagged**.
8	Select the checkbox in the Ingress filtering column for the uplink ports to evaluate VLAN tags on this port.
9	To apply the settings, click the ✓ button.

To set up the VLAN, execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`vlan participation include 1`	The port **1/1** becomes a member of the VLAN **1** and transmits the data packets without a VLAN tag.
`vlan participation include 2`	The port **1/1** becomes a member of the VLAN **2** and transmits the data packets without a VLAN tag.
`vlan tagging 2 enable`	The port **1/1** becomes a member of the VLAN **2** and transmits the data packets with a VLAN tag.
`vlan participation include 3`	The port **1/1** becomes a member of the VLAN **3** and transmits the data packets without a VLAN tag.
`vlan tagging 3 enable`	The port **1/1** becomes a member of the VLAN **3** and transmits the data packets with a VLAN tag.
`vlan pvid 1`	To assign the Port VLAN ID **1** to port **1/1**.
`vlan ingressfilter`	To activate ingress filtering on port **1/1**.
`vlan acceptframe vlanonly`	Port **1/1** only forwards packets with a VLAN tag.
`exit`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface **1/2**.
`vlan participation include 2`	The port **1/2** becomes a member of the VLAN **2** and transmits the data packets without a VLAN tag.
`vlan pvid 2`	To assign the Port VLAN ID **2** to port **1/2**.
`exit`	To change to the Configuration mode.
`interface 1/3`	To change to the Interface Configuration mode of interface **1/3**.
`vlan participation include 3`	The port **1/3** becomes a member of the VLAN **3** and transmits the data packets without a VLAN tag.
`vlan pvid 3`	To assign the Port VLAN ID **3** to port **1/3**.
`exit`	To change to the Configuration mode.
`interface 1/4`	To change to the Interface Configuration mode of interface **1/4**.
`vlan participation include 2`	The port **1/4** becomes a member of the VLAN **2** and transmits the data packets without a VLAN tag.
`vlan pvid 2`	To assign the Port VLAN ID **2** to port **1/4**.
`exit`	To change to the Configuration mode.
`interface 1/5`	To change to the Interface Configuration mode of interface **1/5**.
`vlan participation include 3`	The port **1/5** becomes a member of the VLAN **3** and transmits the data packets without a VLAN tag.
`vlan pvid 3`	To assign the Port VLAN ID **3** to port **1/5**.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.

Command	Description
`show vlan id 3`	To display details for VLAN **3**.

```
VLAN ID......................3
VLAN Name....................VLAN3
VLAN Type....................Static
VLAN Creation Time...........0 days, 00:07:47 (System Uptime)
VLAN Routing.................disabled
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         -         Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         -         Autodetect   Untagged
1/5         Include   Include      Untagged
```

Guest VLAN / Unauthenticated VLAN

A Guest VLAN provides port-based Network Access Control (IEEE 802.1x) to non-802.1x capable supplicants. This feature provides a mechanism to allow unauthorized users to access external networks only. If you connect non-802.1x capable supplicants to an active unauthorized 802.1x port, the supplicants send no responds to 802.1x requests. Since the supplicants send no responses, the port remains in the unauthorized state. The supplicants have no access to external networks.

The Guest VLAN supplicant is a per-port basis configuration. When you set up a Guest VLAN on a port and connect non-802.1x capable supplicants to this port, the device assigns the supplicants to the Guest VLAN. Adding supplicants to a Guest VLAN causes the port to change to the authorized state allowing the supplicants to access to external networks.

An Unauthenticated VLAN provides service to 802.1x capable supplicants which authenticate incorrectly. This function gives unauthorized supplicants access to limited services. If you set up an Unauthenticated VLAN on a port with 802.1x port authentication and the global operation enabled, the device places the port in an Unauthenticated VLAN. When a 802.1x capable supplicant incorrectly authenticates on the port, the device adds the supplicant to the Unauthenticated VLAN. If you also set up a Guest VLAN on the port, non-802.1x capable supplicants use the Guest VLAN.

If the port has an Unauthenticated VLAN assigned, the reauthentication timer counts down. When the time specified in the Reauthentication period [s] column expires and supplicants are present on the port, the Unauthenticated VLAN reauthenticates. When no supplicants are present, the device places the port in the set-up Guest VLAN.

The following example explains how to add a Guest VLAN. Add an Unauthorized VLAN in the same manner.

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **VLAN** > **Configuration**.
2	Click the ⊞ button. The dialog displays the Create window.
3	In the **VLAN ID** field, specify the value **10**.
4	Click **OK**.
5	For the VLAN, specify the name **Guest**: • Double-click the **Name** column and specify the name.
6	Click the ⊞ button. The dialog displays the Create window.
7	In the **VLAN ID** field, specify the value **20**.
8	Click **OK**.
9	For the VLAN, specify the name **Not authorized**: • Double-click the **Name** column and specify the name.
10	Navigate to **Network Security** > **802.1X** > **Global**.
11	• Enable the 802.1X function. • Select the **On** radio button in the Operation frame.
12	To apply the settings, click the ✓ button.
13	Navigate to **Network Security** > **802.1X** > **Port Configuration**.
14	Specify the following settings for port **1/4**: • The value **auto** in the Port control column • The value **10** in the Guest VLAN ID column • The value **20** in the Unauthenticated VLAN ID column
15	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 10`	To add VLAN **10**.
`vlan add 20`	To add VLAN **20**.
`name 10 Guest`	To rename VLAN **10** to **Guest**.
`name 20 Unauth`	To rename VLAN **20** to **Unauth**.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dot1x system-auth-control enable`	To enable the 802.1X function globally.
`dot1x port-control auto`	To enable port control on port **1/4**.
`interface 1/4`	To change to the Interface Configuration mode of interface **1/4**.
`dot1x guest-vlan 10`	To assign the guest vlan to port **1/4**.
`dot1x unauthenticated-vlan 20`	To assign the unauthorized vlan to port **1/4**.
`exit`	To change to the Configuration mode.

RADIUS VLAN Assignment

The RADIUS VLAN assignment feature makes it possible for a RADIUS VLAN ID attribute to be associated with an authenticated client. When a client authenticates successfully, and the RADIUS server sends a VLAN attribute, the device associates the client with the RADIUS assigned VLAN. As a result, the device adds the physical port as a member to the appropriate VLAN and sets the port VLAN ID (PVID) with the given value. The port transmits the data packets without a VLAN tag.

Creating a Voice VLAN

Use the Voice VLAN feature to separate voice and data packets on a port, by VLAN and/or priority. A significant benefit of the voice VLAN is that a high volume of data on the port does not affect the sound quality of an IP phone.

The device uses the source MAC address to identify and prioritize the voice data flow. Identifying by MAC address reduces the potential for a "rogue client" to connect to the port and manipulate voice data packets.

Another benefit of the Voice VLAN feature is that a VoIP phone obtains a VLAN ID or priority information using LLDP-MED. As a result, the VoIP phone sends voice data packets with VLAN tag, priority tag or untagged. This depends on the Voice VLAN Interface configuration.

The following Voice VLAN interface modes are possible. The first 3 methods segregate and prioritize voice and data packets. The segregation of the data packets improves the quality of the voice data stream in case of high data volumes.

- Configuring the port to using the **vlan** mode tags the voice data coming from a VoIP phone with the user-defined voice VLAN ID. The device assigns regular data to the default port VLAN ID.
- Configuring the port to use the **dot1p-priority** mode tags the data coming from a VoIP phone with VLAN 0 and the user-defined priority. The device assigns the default priority of the port to regular data.
- Specify both the voice VLAN ID and the priority using the **vlan/dot1p-priority** mode. In this mode the VoIP phone sends voice data with the user-defined voice VLAN ID and priority information. The device assigns the default PVID and priority of the port to regular data.

  The prerequisite for setting up the priority is that the port does not operate in a private VLAN.
- When set up as **untagged**, the phone sends untagged packets.
- When set up as **none**, the phone uses its own configuration to send voice data packets.

Private VLAN

A private VLAN separates a regular VLAN into 2 or more subdomains. This helps to provide privacy but enables the connected end devices to communicate with the same destination. Each private VLAN has one *primary* VLAN and one or more *secondary* VLANs (*isolated* or *community*).

In a private VLAN, the device controls the data stream between specific ports. The device transmits untagged data packets only. The device allows isolation of the ports within the private VLAN and restrict them from communicating with each other.

Primary and Secondary VLANs

In a private VLAN, the *primary* VLAN is the unique identifier of the entire private VLAN including its *secondary* VLANs. The ports participating in a private VLAN are automatically members of the *primary* VLAN. There are the following types of *secondary* VLANs:

- *isolated*

  The ports you want to be isolated from other ports are members of the *isolated* (*secondary*) VLAN. The ports can communicate with the *promiscuous* port but cannot communicate with each other.
- *community*

  The ports associated with the *community* (*secondary*) VLAN can communicate with the *promiscuous* port as well as with each other.

Port Types

There are the following types of ports in a private VLAN:

- *Promiscuous*

  A *promiscuous* port belongs to the *primary* VLAN. The *promiscuous* port can communicate with each *isolated* and *community* ports that are associated with the private VLAN as well as with other *promiscuous* ports. A private VLAN can contain multiple *promiscuous* ports.
- *Isolated*

  An *isolated* port is associated with an *isolated* VLAN. An *isolated* port can communicate with the *promiscuous* ports. An *isolated* port cannot communicate with other *isolated* or *community* ports.
- *Community*

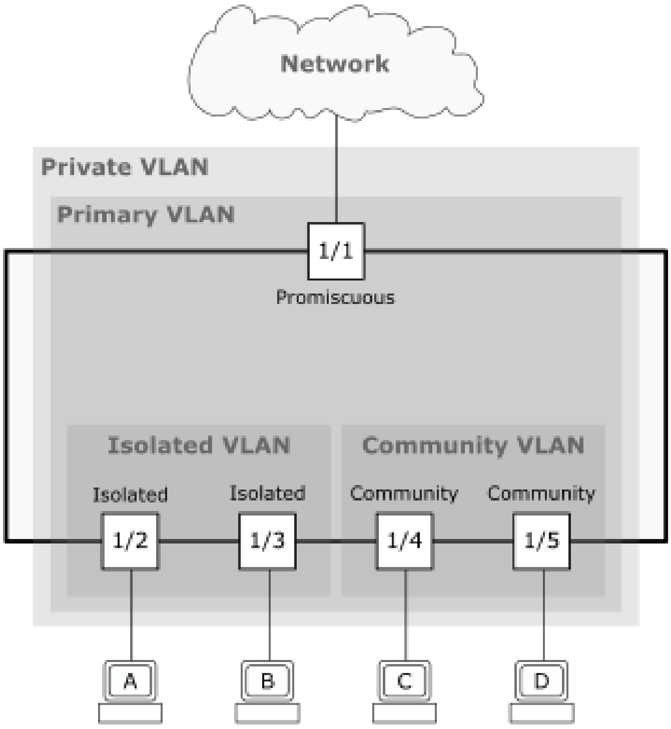
  A *community* port is associated with a *community* VLAN. The *community* port can communicate with the other *community* ports in the same *community* VLAN and with the associated *promiscuous* ports.

If a port operates in a private VLAN, changing the following settings for this port has no effect:

- Port-VLAN ID column, see the **Switching > VLAN > Port** dialog
- Acceptable packet types column, see the **Switching > VLAN > Port** dialog
- Ingress filtering column, see the **Switching > VLAN > Port** dialog
- Priority column, see the **Switching > VLAN > Voice** dialog

Private VLAN Architecture

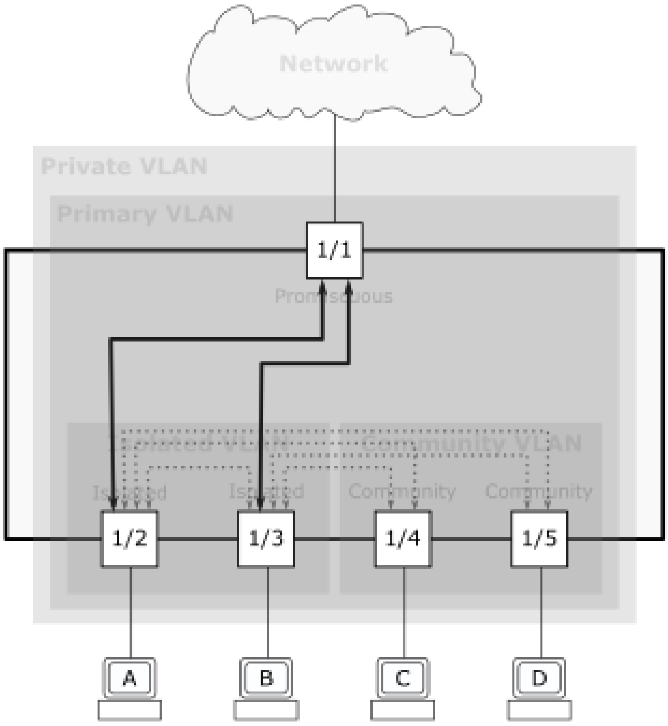
The following figure displays the private VLAN architecture.



The *promiscuous* port can communicate with both the *isolated* ports and with the *community* ports.

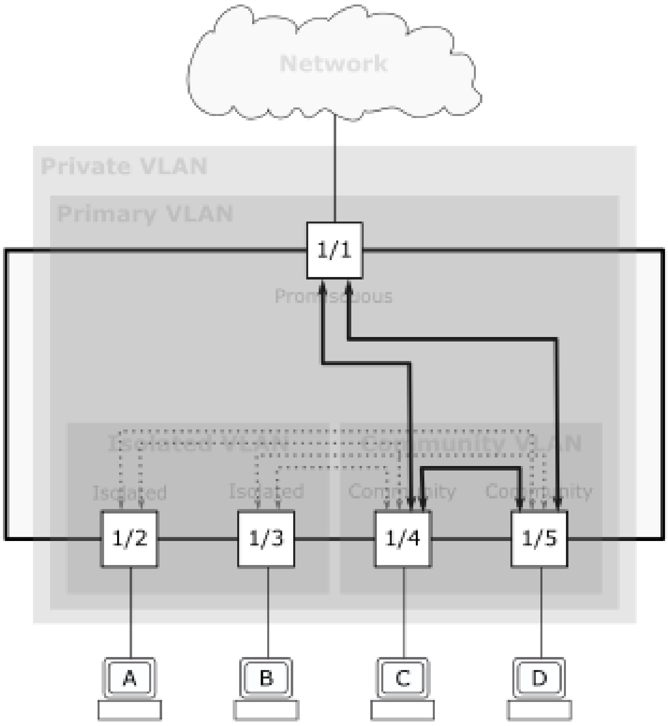
The *isolated* ports **1/2** and **1/3** can communicate with the *promiscuous* port only. For example, if an end device needs to communicate only with a gateway router, connect it to an *isolated* port.

The following figure presents the communication flow of the *isolated* ports:



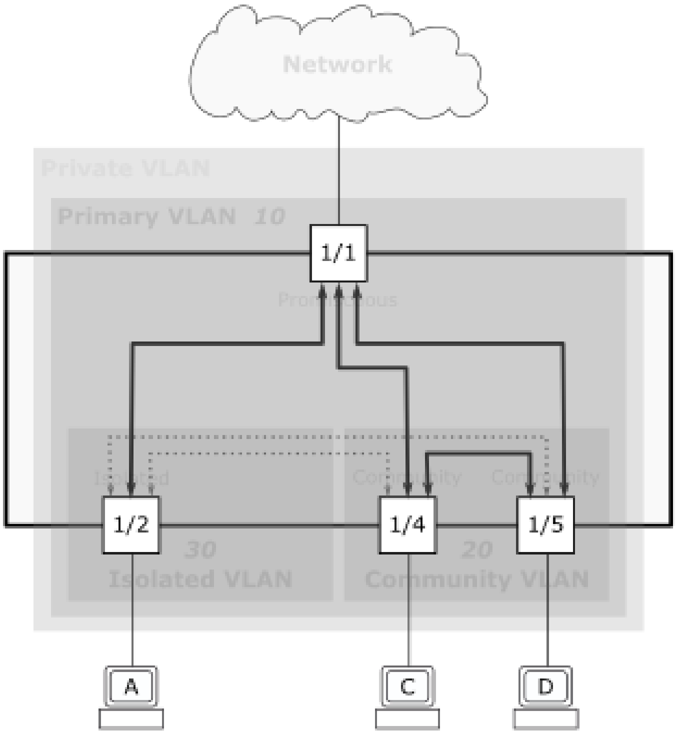
The *community* ports **1/4** and **1/5** can communicate with each other and with the *promiscuous* port. If you have 2 end devices that you want to be isolated from other devices but to be able to communicate with each other, connect these devices to *community* ports.

The following figure presents the communication flow of the *community* ports:



Example Configuration

The following example displays a private VLAN using the 3 VLANs **10**, **20**, and **30**. The prerequisite is that these VLANs are already set up, see the **Switching > VLAN > Configuration** dialog.:



The device allows isolation of the port **1/2** associated with *isolated* VLAN **30**, and ports **1/4** and **1/5** associated with *community* VLAN **20** within the private VLAN. This isolation restricts the ports from communicating with each other. The end devices connected to ports **1/2**, **1/4** and **1/5** can communicate with the device or network connected to port **1/1**.

To set up the private VLAN, specify the *primary* and *secondary* VLANs (*isolated* and *community*) and then associate the *secondary* VLANs with the *primary* VLAN. After that you associate the *promiscuous* port to the *primary* VLAN and the *host* ports to the *secondary* VLANs. To do this, perform the following steps:

Specify the role that the VLAN performs in the private VLAN:

Step	Action
1	Navigate to the **Switching > VLAN > Private VLAN**, **VLAN type** tab.
2	In the VLAN type column, select **primary** for VLAN **10**.
3	In the VLAN type column, select **community** for VLAN **20**.
4	In the VLAN type column, select **isolated** for VLAN **30**.
5	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`private-vlan vlan-id 10 type primary`	To specify the role **primary** for VLAN **10**.
`private-vlan vlan-id 20 type community`	To specify the role **community** for VLAN **20**.
`private-vlan vlan-id 30 type isolated`	To specify the role **isolated** for VLAN **30**.
`exit`	To change to the Privileged EXEC mode.

Associate the *community* and *isolated* VLANs with the *primary* VLAN:

Step	Action
1	Navigate to the **Switching > VLAN > Private VLAN**, **VLAN association** tab.
2	In the Secondary column, select **20 (community)**. You can associate multiple *community* VLANs to a *primary* VLAN.
3	In the Secondary column, select **30 (isolated)**. You can associate only one *isolated* VLAN to a *primary* VLAN.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`private-vlan add associate primary 10 secondary 20`	To associate the *community* VLAN **20** with the *primary* VLAN **10**.
`private-vlan add associate primary 10 secondary 30`	To associate the *isolated* VLAN **30** with the *primary* VLAN **10**.
`exit`	To change to the Privileged EXEC mode.

Specify the role of the ports in the private VLAN:

Step	Action
1	Navigate to the **Switching > VLAN > Private VLAN**, **Port association** tab.
2	For port **1/1**, in the Switchport mode column, select **promiscuous**. This setting allows the port to operate as a *promiscuous* port in the private VLAN.
3	For port **1/2**, in the Switchport mode column, select **host**. This setting allows the port to operate as a *host* port in the private VLAN.
4	For port **1/4**, in the Switchport mode column, select **host**. This setting allows the port to operate as a *host* port in the private VLAN.
5	For port **1/5**, in the Switchport mode column, select **host**. This setting allows the port to operate as a *host* port in the private VLAN.
6	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`switchport mode private-vlan promiscuous`	To specify the port as a **promiscuous** port.
`interface 1/2`	To change to the Interface Configuration mode of interface `1/2`.
`switchport mode private-vlan host`	To specify the port as a **host** port.
`interface 1/4`	To change to the Interface Configuration mode of interface `1/4`.
`switchport mode private-vlan host`	To specify the port as a **host** port.
`interface 1/5`	To change to the Interface Configuration mode of interface `1/5`.
`switchport mode private-vlan host`	To specify the port as a **host** port.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.

Associate the *host* and *promiscuous* ports to the *primary* VLAN and the *secondary* VLANs:

Step	Action
1	Navigate to the **Switching > VLAN > Private VLAN**, **Port association** tab.
2	For port **1/1**, in the Promiscuous primary column, select **10**.
3	For port **1/1**, in the Promiscuous secondary column, select **20 (community)** and **30 (isolated)**.
4	For port **1/2**, in the Host primary column, select **10**.
5	For port **1/2**, in the Host secondary column, select **30**.
6	For port **1/4**, in the Host primary column, select **10**.
7	For port **1/4**, in the Host secondary column, select **20**.
8	For port **1/5**, in the Host primary column, select **10**.
9	For port **1/5**, in the Host secondary column, select **20**.
10	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`switchport private-vlan add promiscuous-association primary 10 secondary 20 30`	To associate *primary* VLAN **10**, *community* VLAN **20** and *isolated* VLAN **30** to the *promiscuous* port.
`interface 1/2`	To change to the Interface Configuration mode of interface `1/2`.
`switchport private-vlan add host-association primary 10 secondary 30`	To associate *primary* VLAN **10** and *isolated* VLAN **30** to the *host* port.
`interface 1/4`	To change to the Interface Configuration mode of interface `1/4`.
`switchport private-vlan add host-association primary 10 secondary 20`	To associate *primary* VLAN **10** and *community* VLAN **20** to the *host* port.
`interface 1/5`	To change to the Interface Configuration mode of interface `1/5`.
`switchport private-vlan add host-association primary 10 secondary 20`	To associate *primary* VLAN **10** and *community* VLAN **20** to the *host* port.
`exit`	To change to the Privileged EXEC mode.
`show vlan private-vlan`	To display the present private VLAN configuration.

```
Primary VLAN Community VLAN Isolated VLAN
------------ ------------- --------------
     10            20            30
```

Command	Description
`show vlan port 1/1`	To display the VLAN configuration of port `1/1`.

```
Port.............................. 1/1
Port VLAN ID....................... 1
Acceptable frame types............ admit all
Ingress filtering................. disable
Priority.......................... 0
Mode.............................. promiscuous
Primary VLAN id................... 10
Association....................... 20,30
```

Command	Description
`show vlan port 1/2`	To display the VLAN configuration of port `1/2`.

```
Port.............................. 1/2
Port VLAN ID....................... 1
Acceptable frame types............ admit all
Ingress filtering................. disable
Priority.......................... 0
Mode.............................. host
Primary VLAN id................... 10
Association....................... 30
```

Command	Description
`show vlan port 1/4`	To display the VLAN configuration of port `1/4`.

```
Port.............................. 1/4
Port VLAN ID....................... 1
Acceptable frame types............ admit all
Ingress filtering................. disable
Priority.......................... 0
Mode.............................. host
Primary VLAN id................... 10
Association....................... 20
```

Command	Description
`show vlan port 1/5`	To display the VLAN configuration of port `1/5`.

```
Port............................. 1/5
Port VLAN ID..................... 1
Acceptable frame types........... admit all
Ingress filtering................ disable
Priority......................... 0
Mode............................. host
Primary VLAN id.................. 10
Association...................... 20
```

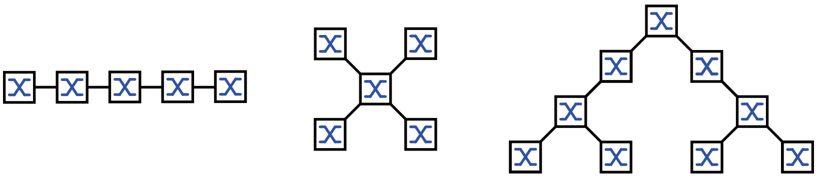
Redundancy

Network Topology vs. Redundancy Protocols

When using Ethernet, a significant prerequisite is that data packets follow a single (unique) path from the sender to the receiver. The following network topologies support this prerequisite:

- Line topology
- Star topology
- Tree topology

The following figure presents networks with line, star and tree topologies



To maintain communication in case a connection interruption is detected, install additional physical connections between the network nodes. Redundancy protocols help ensure that the additional connections remain disabled while the original connection is still operational. When a connection interruption is detected, the redundancy protocol generates a new path from the sender to the receiver through the alternative connection.

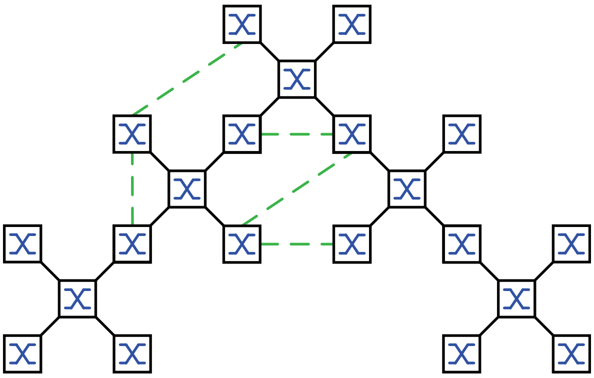
To introduce redundancy onto Layer 2 of a network, you first define which network topology you require. Depending on the network topology selected, you then choose from the redundancy protocols that can be used with this network topology.

Network Topologies

Meshed Topology

For networks with star or tree topologies, redundancy procedures are only possible in connection with physical looping. The result is a meshed topology.

The following figure presents meshed topology containing the tree topology with physical loops:



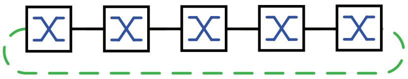
For operating in this network topology, the device provides you with the following redundancy protocols:

- Rapid Spanning Tree Protocol (RSTP)

Ring Topology

In networks with a line topology, you can use redundancy procedures by connecting the ends of the line. This results in a ring topology.

The following figure presents ring topology containing line topology with connected ends:



For operating in this network topology, the device provides you with the following redundancy protocols:

- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree Protocol (RSTP)

Redundancy Protocols

For operating in different network topologies, the device provides you with the following redundancy protocols:

Redundancy protocol	**Network topology**	**Comments**
MRP	Ring	The switching time can be selected and is practically independent of the number of devices. An MRP Ring consists of up to 50 devices that support the Media Redundancy Protocol (MRP) according to IEC 62439. When you only use Schneider Electric devices, up to 100 devices are possible in the MRP Ring.
Sub Ring	Ring	The Sub Ring function allows coupling network segments to existing redundancy rings.
Ring/Network coupling	Ring	
RCP	Ring	
RSTP	Random structure	The switching time depends on the network topology and the number of devices. • typically < 1 s with RSTP • typically < 30 s with STP
Link Aggregation	Random structure	A Link Aggregation Group (LAG) is a combination of 2 or more links between 2 switches to increase bandwidth. Each involved link operates in full-duplex mode and with the same data rate.
Link Backup	Random structure	When the device detects an error on the primary link, the device transfers the data packets to the backup link. You typically use Link Backup in service-provider or enterprise networks.
HIPER Ring Client	Ring	Extend an existing HIPER Ring or replace a device already participating as a client in a HIPER Ring.
HIPER Ring over LAG	Ring	Link devices together over a Link Aggregation Group (LAG). The *Ring Manager* and *Ring Client* devices behave in the same manner as a ring without a LAG instance.

If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

Deactivate the flow control on the participating ports if you are using a redundancy function.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Combinations of Redundancy Protocols

The following table presents an overview of redundancy protocol combinations:

	MRP	RSTP/ MSTP	Link Aggregation	Link Backup	Sub Ring	HIPER Ring
MRP	x	–	–	–	–	–
RSTP/ MSTP3)	x[1]	x	–	–	–	–
Link Aggregation	x[2]	x[2]	x	–	–	–
Link Backup	x	x	x	x	–	–
Sub Ring	x	x	x[2]	x	x	–
HIPER Ring	x	x[1]	x[2]	x	x	x

[1] A redundant coupling between these network topologies will possibly lead to loops. To redundantly couple these topologies, refer to FuseNet Function, page 219.

[2] The combination is applicable on the same port.

[3] In combination with MSTP, the switchover time of other redundancy protocols can slightly increase.

x The combination is applicable.

– The combination is not applicable.

Media Redundancy Protocol (MRP)

Since May 2008, the Media Redundancy Protocol (MRP) has been a standardized solution for ring redundancy in the industrial environment.

MRP is compatible with redundant ring coupling, supports VLANs, and is distinguished by very short reconfiguration times.

An MRP Ring consists of up to 50 devices that support the Media Redundancy Protocol (MRP) according to IEC 62439. When you only use Schneider Electric devices, up to 100 devices are possible in the MRP Ring.

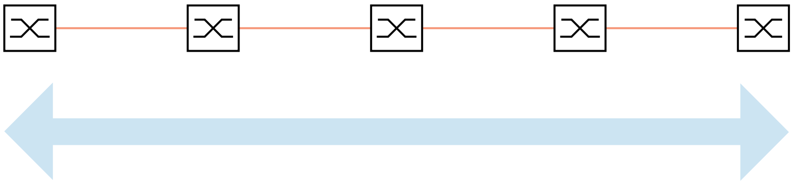
When you use the fixed MRP redundant port (Fixed Backup) and the *Ring Manager* device detects a primary ring link error, it forwards data to the secondary ring link. When the primary link is restored, the secondary link continues to be in use.

Network Structure

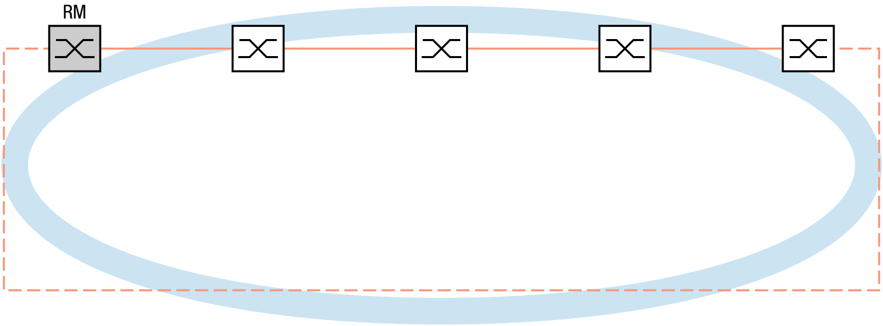
The concept of ring redundancy allows high-availability ring-shaped network structures.

Using the Ring manager function, the two ends of a backbone in a line structure can be closed to a redundant ring. The *Ring Manager* device keeps the redundant line open as long as the line structure is intact. When a segment becomes inoperable, the *Ring Manager* device immediately closes the redundant line, and line structure is intact again.

The following figure presents the line structure:



The following figure presents the redundant ring structure:



RM: Ring Manager
——: Main line
- - -: Redundant line

Reconfiguration Time

When a line section error is detected, the *Ring Manager* device changes the MRP Ring back into a line structure. You define the maximum time for the reconfiguration of the line in the *Ring Manager* device.

Possible values for the maximum delay time:

- **500ms**
- **30ms**

  NOTE: If every device in the ring supports the shorter delay time, you can set up the reconfiguration time with a value less than **500ms**. Otherwise the devices that only support longer delay times might not be reachable due to overloading. Loops can occur as a result.

Advanced mode

For times even shorter than the specified reconfiguration time, the device provides the *Advanced mode*. When the ring participants inform the *Ring Manager* device about interruptions in the ring through *Link Down* notifications, the *Advanced mode* speeds up the link error detection.

Schneider Electric devices support *Link Down* notifications. Therefore, you generally activate the *Advanced mode* in the *Ring Manager* device.

When you are using devices that do not support *Link Down* notifications, the *Ring Manager* device reconfigures the line in the selected maximum reconfiguration time.

Prerequisites for MRP

Before setting up an MRP Ring, verify that the following conditions are fulfilled:

- All ring participants support MRP.
- The ring participants are connected to each other through the ring ports. Apart from its neighbors, no other ring participants are connected to the respective device.
- All ring participants support the configuration time specified in the *Ring Manager* device.
- There is exactly one *Ring Manager* device in the ring.

If you are using VLANs, set up every ring port with the following settings:

- Deactivate ingress filtering - see the **Switching > VLAN > Port** dialog.
- Define the port VLAN ID (PVID) - see the **Switching > VLAN > Port** dialog.
  - PVID = **1** in cases where the device transmits the MRP data packets untagged (VLAN ID = **0** in **Switching > L2-Redundancy > MRP** dialog)

    By setting the PVID = **1**, the device automatically assigns the received untagged packets to VLAN 1.
  - PVID = **any** in cases where the device transmits the MRP data packets in a VLAN (VLAN ID ≥**1** in the **Switching > L2-Redundancy > MRP** dialog)
- Define egress rules - see **Switching > VLAN > Configuration** dialog.
  - **U** (untagged) for the ring ports of VLAN 1 in cases where the device transmits the MRP data packets untagged (VLAN ID = **0** in the **Switching > L2-Redundancy > MRP** dialog, the MRP Ring is not assigned to a VLAN).
  - **T** (tagged) for the ring ports of the VLAN which you assign to the MRP Ring. Select **T**, in cases where the device transmits the MRP data packets in a VLAN (VLAN ID ≥**1** in the **Switching > L2-Redundancy > MRP** dialog).

Advanced Information

MRP Packets

The Media Redundancy Protocol (MRP) uses *Test*, *Link Change*, and *Topology Change* (*FDB Flush*) packets.

The *Ring Manager* device is connected to the ring with 2 ring ports. As long as all connections in the ring are operational, the *Ring Manager* device sets one of its ports, the redundant port, into the *blocking* state. In this state, the redundant port neither receives nor sends normal (payload) data packets. This way, the *Ring Manager* device helps prevent a network loop.

The *Ring Manager* device periodically sends test packets into the ring from both ring ports. The test packets are special packets. The *Ring Manager* device sends and receives test packets even at the redundant port although the redundant port blocks normal packets. The *Ring Manager* device expects to receive the test packets on its respective other ring port. If the *Ring Manager* device does not receive any expected test packets for a specified amount of time, it detects a ring interruption.

If the Advanced mode function is active, the *Ring Manager* device also reacts to *Link Down* packets. The prerequisite is that each device in the ring can send a *Link Change* packet when the link to the next device in the ring changes. These packets help the *Ring Manager* device react to a link interruption or recovery. The *Ring Manager* device receives the *Link Change* packets even on its redundant port.

On reconfiguration of the ring, the *Ring Manager* device flushes its MAC address table (forwarding database) and sends *Topology Change* packets to the devices participating in the ring. The *Topology Change* packets also prompt the other devices participating in the ring to flush their MAC address table (forwarding database). This procedure helps forward the payload packets over the new path. This procedure applies regardless of whether the ring reconfiguration was caused by a *Link Down* or a *Link Up* notification.

The following table describes MRP packets:

Packet Type	Send Mode	Time Parameter	Value
Test packet[1]	Periodically	Send interval	50 ms (for ring recovery time 500 ms) 20 ms (for ring recovery time 200 ms)
		Reception timeout	400 ms (for ring recovery time 500 ms) 160 ms (for ring recovery time 200 ms)
Link Down packet[2]	Event-driven	On link-down of a ring port	-
Topology Change packet[3]	Event-driven	On reconfiguration	-

MRP Packet Prioritization

The devices participating in the ring send *Test*, *Link Change*, and *Topology Change* packets with a user-configurable VLAN ID. The default VLAN ID is 0. The devices send the test packets untagged and thus without priority (Class of Service) information.

To help minimize the reconfiguration time under high network load, you can add a VLAN tag and thus priority information to these packets. The devices then forward and send these packets with the IEEE 802.1Q Class of Service priority 7 (Network control).

To prioritize the test packets, perform the following steps on the *Ring Manager* and *Ring Client* devices:

- Specify the MRP VLAN ID to a value ≥**1**.
- Specify the ring ports as **T** (tagged) members of this MRP VLAN.

  NOTE: When you set the MRP VLAN ID to a value ≥**1** in the **Switching > L2-Redundancy > MRP** dialog, the device adds its ring ports as **T** (tagged) members of this MRP VLAN. If the MRP VLAN does not yet exist, the device automatically sets up this VLAN. After setting a new MRP VLAN ID, verify the **Switching > VLAN > Configuration** dialog for the VLAN and the port settings.

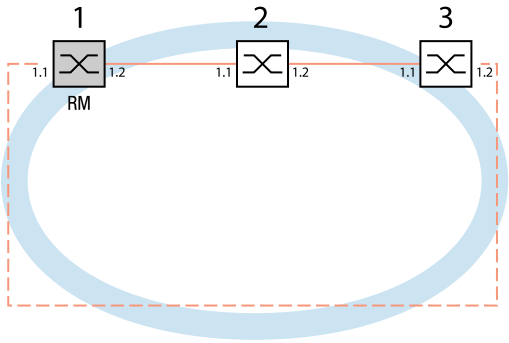
Application Example of an MRP Ring

A backbone network contains 3 devices in a line structure. To increase the availability of the network, you convert the line structure to a redundant ring structure. Devices from different manufacturers are used. All devices support MRP. On every device you define ports ***1/1*** and ***1/2*** as ring ports.

When a primary ring link error is detected, the *Ring Manager* device sends data on the secondary ring link. When the primary link is restored, the secondary link reverts back to the backup mode.

[1] Sent by the *Ring Manager* device only.
[2] Sent by supporting ring participants.
[3] The reception of a *Topology Change* packet prompts the supporting devices participating in the ring to flush their MAC address table (forwarding database).

The following figure presents an example of the MRP Ring:



RM: Ring Manager
——: Main line
- - -: Redundant line

The following example configuration describes the configuration of the *Ring Manager* device (1). You set up the 2 other devices (2 to 3) in the same way, but without enabling the Ring manager function. This example does not use a VLAN. You specify the value **30ms** as the ring recovery time. Every device supports the Advanced mode function.

- Set up the network to meet your demands.
- To minimize the ring recovery time in case of a link-up after an interruption, set up the speed and duplex mode of the ring ports as follows:
  - For 100 Mbit/s TX ports, disable Automatic Negotiation and manually set up 100M FDX.
  - For the other port types, keep the port-specific default settings.

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the MRP configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

You deactivate the flow control on the participating ports.

If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended. (Default setting: flow control deactivated globally and activated on every port.)

Disable the Spanning Tree function in every device in the network. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching** > **L2-Redundancy** > **Spanning Tree** > **Global**.
2	Disable the function. In the state on delivery, Spanning Tree is enabled in the device.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no spanning-tree operation`	To switch Spanning Tree off.
`show spanning-tree global`	To display the parameters for verifying.

Enable MRP on every device in the network. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching > L2-Redundancy > MRP**.
2	Specify the desired ring ports.

In the Command Line Interface you first define an additional parameter, the MRP domain ID. Set up every ring participant with the same MRP domain ID. The MRP domain ID is a sequence of 16 number blocks (8-bit values).

When configuring with the Graphical User Interface, the device uses the default value **255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255**.

Execute the following commands:

Command	Description
`mrp domain add default-domain`	To add an MRP domain with the ID ***default-domain***.
`mrp domain modify port primary 1/1`	To specify port ***1/1*** as ring port **1**.
`mrp domain modify port secondary 1/2`	To specify port ***1/2*** as ring port **2**.

Enable the Fixed backup port. To do this, perform the following steps:

Step	Action
1	Enable the Ring manager function. For the other devices in the ring, leave the setting as **Off**.
2	To allow the device to continue sending data on the secondary port after the ring is restored, select the Fixed backup checkbox. **NOTE:** When the device reverts back to the *Primary port*, the maximum ring recovery time can be exceeded. When you clear the Fixed backup checkbox, and the ring is restored, the *Ring Manager* device blocks the secondary port and unblocks the *Primary port*.
3	To activate the Fixed backup function on the secondary port. Execute the following command: `mrp domain modify port secondary 1/2 fixed-backup enable` The secondary port continues forwarding data after the ring is restored.
4	Enable the Ring manager function. For the other devices in the ring, leave the setting as **Off**.
5	To designate the device as the *Ring Manager* device, execute the following command: `mrp domain modify mode   manager` For the other devices in the ring, use the default setting.
6	Select the checkbox in the **Advanced mode** field.
7	To activate the *Advanced mode*, execute the following command: `mrp domain modify   advanced-mode enabled`
8	In the **Ring recovery** field, select the value **30ms**.
9	To specify the value **30ms** as the max. delay time for the reconfiguration of the ring, execute the following command: `mrp domain modify   recovery-delay 200ms` **NOTE:** If selecting the value **30ms** for the ring recovery does not provide the ring stability necessary to meet the requirements of the network, select the value **500ms**.
10	Switch the operation of the MRP Ring on.
11	To apply the settings, click the ✓ button.
12	To activate the MRP Ring, execute the following command: `mrp domain modify operation   enable`

When every ring participant is set up, close the line to create the ring. To do this, you connect the devices at the ends of the line through their ring ports.

Verify the messages from the device. To display the parameters for verifying., execute the following command:

```
show mrp
```

The **Operation** field displays the operating state of the ring port.

Possible values:

- **forwarding**

  The port is enabled, connection exists.
- **blocked**

  The port is blocked, connection exists.
- **disabled**

  The port is disabled.
- **not-connected**

  No connection exists.

The **Information** field displays messages for the redundancy configuration and the possible causes of detected errors.

When the device operates in the *Ring Client* or *Ring Manager* mode, the following messages are possible:

- Redundancy available. Ring is closed.

  The redundancy is set up. When a component of the ring is inoperable, the redundant line takes over its function.
- Configuration error: Error on ring port link.

  An error is detected in the cabling of the ring ports.

When the device operates in the *Ring Manager* mode, the following messages are possible:

- Configuration error: Packets from another ring manager received.

  Another device exists in the ring that operates in the *Ring Manager* mode.

  Enable the Ring manager function on exactly one device in the ring.
- Configuration error: Ring link is connected to undefined port.

  A line in the ring is connected with a different port instead of with a ring port. The device only receives test data packets on one ring port.

When applicable, integrate the MRP Ring into a VLAN. To do this, perform the following steps:

Step	Action
1	In the **VLAN ID** field, define the MRP VLAN ID. The MRP VLAN ID determines in which of the set-up VLANs the device transmits the MRP packets.
2	To set the MRP VLAN ID, first set up the VLANs and the corresponding egress rules in the **Switching > VLAN > Configuration** dialog. • If the MRP Ring is not assigned to a VLAN (like in this example), leave the VLAN ID as **0**. In the **Switching > VLAN > Configuration** dialog, specify the VLAN membership as **U** (untagged) for the ring ports in VLAN **1**. • If the MRP Ring is assigned to a VLAN, enter a VLAN ID >**0**. In the **Switching > VLAN > Configuration** dialog, specify the VLAN membership as **T** (tagged) for the ring ports in the selected VLAN.
3	To assign the VLAN ID, execute the following command: `mrp domain modify vlan  <0..4042>`

MRP over LAG

Schneider Electric devices let you combine *Link Aggregation Groups (LAG)* to increase bandwidth with the Media Redundancy Protocol (MRP) providing redundancy. The function allows bandwidth increase on individual segments or on the entire network.

The Link Aggregation function helps you overcome bandwidth limitations of individual ports. LAG allows two or more connections into one logical connection between 2 devices. The parallel links increase the bandwidth between the 2 devices.

An MRP Ring consists of up to 50 devices that support the Media Redundancy Protocol (MRP) according to IEC 62439. When you use only Schneider Electric devices, the protocol allows MRP Rings with up to 100 devices.

You use MRP over LAG in the following cases:

- to increase bandwidth only on specific segments of an MRP Ring
- to increase bandwidth on the entire MRP Ring

Network Structure

When configuring an MRP Ring with LAGs, the *Ring Manager* device monitors both ends of the backbone for continuity. The *Ring Manager* device blocks data on the secondary (redundant) port as long as the backbone is intact. When the *Ring Manager* device detects an interruption of the data stream on the ring, it begins forwarding data on the secondary port, which restores backbone continuity.

You use LAG instances in MRP Rings to increase bandwidth only, in this case MRP provides the redundancy.

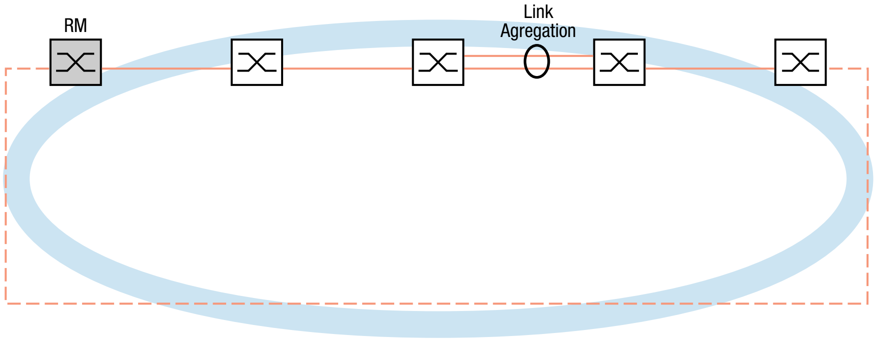
For the *Ring Manager* device to detect an interruption on the ring, MRP requires a device to block every port in the LAG instance in cases where a port in the instance is down.

LAG on a Single Segment of an MRP Ring

The device allows a LAG instance on individual segments of an MRP Ring.

You use the LAG Single Switch method for devices in the MRP Ring. The Single Switch method provides you an inexpensive way to grow the network by using only one device on each side of a segment to provide the physical ports. You group the ports of the device into a LAG instance to provide increased bandwidth on specific segments where needed.

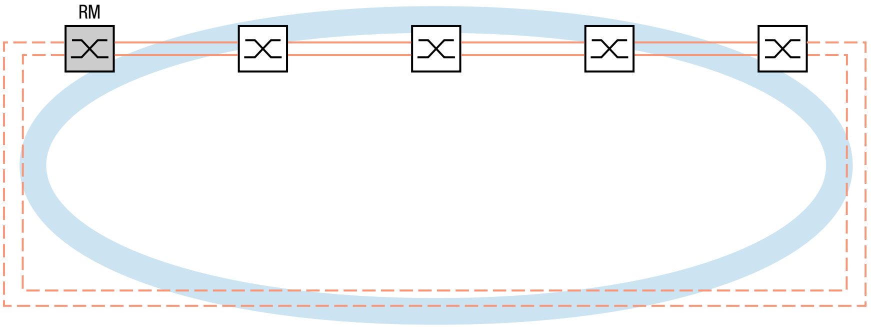
The following figure presents the Link Aggregation over a single link of an MRP Ring:



LAG on an Entire MRP Ring

Besides being able to set up a LAG instance on specific segments of an MRP Ring, Schneider Electric devices also allow you to set up LAG instances on every segment, which increases bandwidth on the entire MRP Ring.

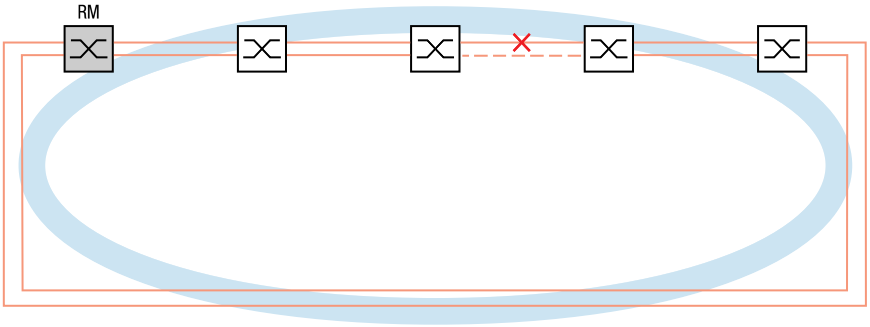
The following figure presents the Link Aggregation over the entire MRP Ring:



Detecting Interruptions on the Ring

When configuring the LAG instance, specify the Active ports (min.) value to equal the total number of ports used in the LAG instance. When a device detects an interruption on a port in the LAG instance, it blocks data on the other ports of the instance. With every port of an instance blocked, the *Ring Manager* device detects that the ring is open and begins forwarding data on the secondary port. This way the *Ring Manager* device can restore continuity to the devices on the other side of the interrupted segment.

The following figure presents the interruption of a link in an MRP Ring:

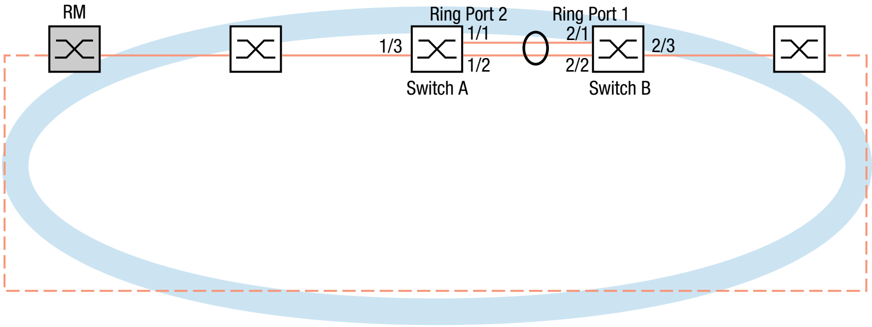


Application example for MRP over LAG

In the following example, switch A and switch B link two departments. The data volume of the departments exceeds the individual bandwidth capacity of the ports. You set up an LAG instance for the single segment of the MRP Ring, increasing the bandwidth of the segment.

The prerequisite for the example configuration is that you begin with an operational MRP Ring.

The following figure presents an application example of an MRP over LAG setup:



Set up the switch A first. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching** > **L2-Redundancy** > **Link Aggregation**.
2	Click the + button. The dialog displays the Create window.
3	From the Trunk port drop-down list, select the instance number of the link aggregation group.
4	From the Port drop-down list, select port ***1/1***.
5	Click **OK**.
6	Repeat the preceding steps and select the port ***1/2***.
7	Click **OK**.
8	In the Active ports (min.) column enter **2**, which in this case is the total number of ports in the instance. When combining MRP and LAG you specify the total number of ports as the Active ports (min.). When the device detects an interruption on a port, it blocks the other ports in the instance causing the ring to open. The *Ring Manager* device detects that the ring is open, then begins forwarding data on its secondary ring port which restores the connectivity to the other devices in the network.
9	To apply the settings, click the ✓ button.
10	Navigate to **Switching** > **L2-Redundancy** > **MRP**.
11	In the Ring port 2 frame, select port **lag/1** from the Port drop-down list.
12	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`link-aggregation add lag/1`	To add a Link Aggregation Group **lag/1**.
`link-aggregation modify lag/1 addport 1/1`	To add port ***1/1*** to the Link Aggregation Group.
`link-aggregation modify lag/1 addport 1/2`	To add port ***1/2*** to the Link Aggregation Group.
`mrp domain modify port secondary lag/1`	To specify port **lag/1** as ring port **2**.
`copy config running-config nvm`	To save the updated settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Set up the switch B using the same steps, substituting the appropriate port and ring port numbers.

HIPER Ring Client

The concept of HIPER Ring Redundancy enables the construction of high-availability, ring-shaped network structures. The HIPER Ring Client function allows you extend an existing HIPER Ring or replace a client device already participating in a HIPER Ring.

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the HIPER Ring configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

When the device senses that the link on a ring port becomes inoperable, the device sends a *Link Down* packet to the *Ring Manager* device and flushes the MAC address table (forwarding database). As soon as the *Ring Manager* device receives the *Link Down* packet, it immediately forwards the data stream over both the primary and secondary ring ports. Thus, the *Ring Manager* device can maintain the integrity of the HIPER Ring.

The device only supports Fast Ethernet and Gigabit Ethernet ports as ring ports. Furthermore, you can include the ring ports in a LAG instance.

In the default state, the *HIPER Ring Client* mode is inactive, and the primary and secondary ports are not set up.

To minimize the ring recovery time in case of a link-up after an interruption, set up the speed and duplex mode of the ring ports as follows:

- For 100 Mbit/s TX ports, disable Automatic Negotiation and manually specify 100M FDX.
- For the other port types, keep the port-specific default settings.

NOTE: Deactivate in the **Switching > L2-Redundancy > Spanning Tree > Port** dialog the Spanning Tree function for the ring ports. STP and HIPER Ring have different reaction times.

VLANS on the HIPER Ring

The device allows you to forward VLAN data over the HIPER Ring. Thus, the device provides redundancy for your VLAN data. The device forwards management data around the ring, for example, on VLAN 1. For the data to reach the PC, the devices participating in the ring forward the untagged management data to their ring ports. Also, specify the ring ports as members of VLAN 1.

When you have other VLANs traversing your ring, the devices participating in the ring forward the other VLAN data as tagged.

Specify the VLAN settings. To do this, perform the following steps on the *Ring Manager* and *Ring Client* devices:

Step	Action
1	Navigate to **Switching > VLAN > Configuration**.
2	Forward untagged VLAN management data on the ring ports. For VLAN 1, select **U** from the drop down list in the columns related to the ring ports.
3	Block redundancy protocol packets from being forwarded to the non-ring ports: For VLAN 1, select **-** from the drop-down list in the columns that are **not** related to the ring ports.
4	Allow a device participating in the ring to forward VLAN data to and from ports with VLAN membership. For the other VLANs, select **T** from the drop-down list in the columns related to the ring ports.
5	Navigate to **Switching > VLAN > Port**.
6	Assign VLAN 1 membership to the ring ports. Enter the value **1** in the Port-VLAN ID column of the ring port rows.
7	Assign VLAN membership to the non-ring ports. Enter the appropriate VLAN ID in the Port-VLAN ID column of the non-ring port rows.

Advanced Information

The HIPER Ring is the proprietary predecessor of MRP. The HIPER Ring works similar to MRP but uses different packets. For setting up a new redundant ring, use MRP.

HIPER Ring Packets

The HIPER Ring protocol uses *Test*, *Link Down*, and *Topology Change* packets.

The *Ring Manager (RM)* device is connected to the ring with 2 ring ports. As long as all connections in the ring are operational, the *Ring Manager* device sets one of its ports, the redundant port, into the *blocking* state. In this state, the redundant port neither receives nor sends normal (payload) data packets. This way, the *Ring Manager* device helps prevent a network loop.

The *Ring Manager* device periodically sends test packets into the ring from both ring ports. The test packets are special packets. The *Ring Manager* device sends and receives test packets even at the redundant port although the redundant port blocks normal packets. The *Ring Manager* device expects to receive the test packets on its respective other ring port. If the *Ring Manager* device does not receive any expected test packets for a specified amount of time, it detects a ring interruption.

When a link between 2 devices participating in the ring becomes inoperable, the affected devices send a *Link Down* packet to the *Ring Manager* device. This helps the *Ring Manager* device react to a link interruption. The *Ring Manager* device receives the *Link Down* packets even on its redundant port.

On reconfiguration of the ring, the *Ring Manager* device flushes its MAC address table (forwarding database) and sends *Topology Change* packets to the devices participating in the ring. The *Topology Change* packets also prompt the other devices participating in the ring to flush their MAC address table (forwarding database). This procedure helps forward the payload packets over the new path. This procedure applies regardless of whether the ring reconfiguration was caused by a *Link Down* or a *Link Up* notification.

The following table describes the HIPER Ring Packets:

Packet type	Send mode	Time parameter	Value
Test packet[1]	Periodically	Send interval[2]	20 ms (Ring recovery time accelerated) 60 ms (Ring recovery time standard)
		Reception timeout	280 ms (Ring recovery time accelerated) 480 ms (Ring recovery time standard)
Link Down packet[3]	Event-driven	On link-down of a ring port	–
Topology Change packet[4]	Event-driven	On reconfiguration	–

[1] Sent by the *HIPER Ring Manager* device (Classic Software) only.

[2] Specified in the *HIPER Ring Manager* device (Classic Software) only.

[3] Sent by supporting ring participants.

[4] The reception of a *Topology Change* packet prompts the supporting devices participating in the ring to flush their MAC address table (forwarding database).

HIPER Ring Packet Prioritization

The devices participating in the ring send *Test*, *Link Change*, and *Topology Change* packets with the fixed VLAN ID 1. In the default setting, these packets are untagged and thus without priority (Class of Service) information. To help minimize the reconfiguration time under high network load, you can add a VLAN tag and thus priority information to these packets. The *Ring Manager* and *Ring Client* devices then forward and send these packets with the IEEE 802.1Q Class of Service priority 7 (Network control).

To do that, specify on the *Ring Manager* device (Classic software) and *Ring Client* devices the ring ports as **T** (tagged) members of VLAN 1.

> **NOTE:** These settings for VLAN 1 are different from the VLAN settings described in chapter VLANS on the HIPER Ring, page 196.

HIPER Ring over LAG

The HIPER Ring function allows you to link the devices together over a Link Aggregation Group (LAG). The *Ring Manager* and *Ring Client* devices behave in the same manner as a ring without a LAG instance.

If an LAG link goes down, the other link in the instance also goes down making a break in the ring. After detecting a break in the ring, the affected ports send a *Link Down* packet to the *Ring Manager* device. The *Ring Manager* device unblocks its redundant port, sends data in both directions in the ring, and replies with a *Topology Change* packet. Upon receiving a *Topology Change* packet, the ring participants flush their MAC address table (forwarding database).

Spanning Tree

Local networks are getting bigger and bigger. This applies to both the geographical expansion and the number of network participants. Therefore, it is advantageous to use multiple bridges, for example:

- To reduce the network load in sub-areas,
- To set up redundant connections and
- To overcome distance limitations.

NOTE: The Spanning Tree Protocol (STP) is a protocol for MAC bridges. For this reason, the present description uses the term bridge for the device.

However, using multiple bridges with multiple redundant connections between the subnets can lead to loops and thus interruption of communication across the network. To help avoid this, you can use Spanning Tree. Spanning Tree helps avoid loops through the systematic deactivation of redundant connections. Redundancy enables the systematic reactivation of individual connections as needed.

RSTP is a further development of the Spanning Tree Protocol (STP) and is compatible with it. When a connection or a bridge becomes inoperable, the STP requires a maximum of 30 seconds to reconfigure. This is no longer acceptable in time-sensitive applications. RSTP achieves average reconfiguration times of less than a second. When you use RSTP in a ring topology with 10 to 20 devices, you can even achieve reconfiguration times in the order of milliseconds.

NOTE: RSTP reduces a layer 2 network topology with redundant paths into a tree structure (Spanning Tree) that does not contain any more redundant paths. One of the devices takes over the role of the *Root bridge* here. The maximum number of devices permitted in an active branch from the *Root bridge* to the tip of the branch is specified by the variable Max age for the *Root bridge*. The preset value for Max age is **20**, which can be increased up to **40**. If the device working as the root is inoperable and another device takes over its function, the Max age setting of the new *Root bridge* determines the maximum number of devices allowed in a branch.

NOTE: The RSTP standard requires that every device within a network operates with the (Rapid) Spanning Tree Algorithm. When STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost in the network segments that are operated in combination.
A device that only supports RSTP works together with MSTP devices by not assigning an MST region to itself, but rather the Common Spanning Tree (CST).

Basics

Because RSTP is a further development of the STP, every of the following descriptions of the STP also apply to RSTP.

The Tasks of the STP

The Spanning Tree Algorithm reduces network topologies built with bridges and containing ring structures due to redundant links to a tree structure. In doing so, STP opens ring structures according to preset rules by deactivating redundant paths. When a path is interrupted because a network component becomes inoperable, STP reactivates the previously deactivated path again. This allows redundant links to increase the availability of communication.

STP determines a bridge that represents the STP tree structure‘s base. This bridge is called *Root bridge*.

Features of the STP algorithm:

- Automatic reconfiguration of the tree structure in the case of a bridge becoming inoperable or the interruption of a data path.
- The tree structure is stabilized up to the maximum network size.
- The topology stabilizes within a predictable time period.
- The administrator can specify and reproduce the topology.
- Transparency for the end devices.
- The network load is low relative to the available transmission capacity due to the tree structure set-up.

Bridge Parameters

In the context of Spanning Tree, each bridge and its connections are uniquely described by the following parameters:

- *Bridge Identifier*
- *Root path cost* of the bridge ports
- *Port Identifier*

Bridge Identifier

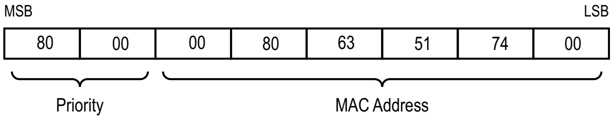
The *Bridge Identifier* consists of 8 bytes. The bridge with the numerically lowest *Bridge Identifier* value has the highest priority.

According to the original standard IEEE 802.1D-1998, the 2 highest-value bytes are the *Bridge priority*. When configuring the bridge, the bridge administrator can change the default setting for the *Bridge priority* which is **32768** (8000H).

In the newer standard IEEE 802.1Q-2014, the *Bridge priority* is interpreted differently. The highest 4 bits represent the *Bridge priority*. The lower 12 bits are reserved for the VLAN ID and are all zero. As a result, the bridge administrator can set the *Bridge priority* in steps of 4096. The default value is **32768** (8000H), and the max. value is **61440** (F000H).

The six lowest-value bytes of the *Bridge Identifier* are the MAC address of the bridge. The MAC address allows each bridge to have a unique *Bridge Identifier*.

The following figure presents an example of the *Bridge Identifier* (an interpretation according to IEEE 802.1D-1998, the values are in hexadecimal notation)

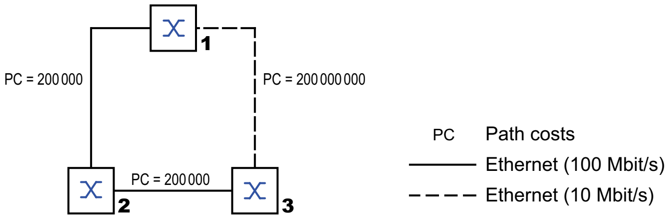


Root path cost

Each path that connects two bridges is assigned a cost for the transmission (path cost). The device determines this value based on the transmission speed. Refer to the table hereafter for the typical path costs for RSTP based on the data rate. The device assigns a greater path cost to paths with lower transmission speeds.

As an alternative, the administrator can set the path cost. Like the device, the administrator assigns a greater path cost to paths with lower transmission speeds. However, since the administrator can choose this value freely, he/she has a tool with which he/she can give a certain path an advantage among redundant paths.

The *Root path cost* is the sum of the individual path cost from the port of the connected bridge to the *Root bridge*:



The table below presents typical path costs for RSTP based on the data rate:

Data rate	Typical value	Typical range	Possible range
≤100 kbit/s	200 000 000[1]	20 000 000-200 000 000	1-200 000 000
1 Mbit/s	20 000 000[a]	2 000 000-200 000 000	1-200 000 000
10 Mbit/s	2 000 000[a]	200 000-20 000 000	1-200 000 000

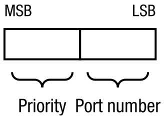
Data rate	Typical value	Typical range	Possible range
100 Mbit/s	200 000[a]	20 000-2 000 000	1-200 000 000
1 Gbit/s	20 000	2 000-200 000	1-200 000 000
10 Gbit/s	2 000	200-20 000	1-200 000 000
100 Gbit/s	200	20-2 000	1-200 000 000
1 Tbit/s	20	2-200	1-200 000 000
10 Tbit/s	2	1-20	1-200 000 000
[1] Verify that bridges, which conform to IEEE 802.1D-1998 and only support 16-bit values for the path cost, use the value 65535 (FFFFH) for path costs in cases where they are used in conjunction with bridges that support 32-bit values for the path costs.			

Port Identifier

According to the original standard IEEE 802.1D-1998, the *Port Identifier* consists of 2 bytes. The lower-value byte contains the physical port number. This provides a unique identifier for the port of this bridge. The greater-value byte is the *Port priority*, which is specified by the administrator (default value: **128** or 80H).

In the newer standard IEEE 802.1Q-2014, the *Port priority* is interpreted differently. The greater 4 bits represent the *Port priority*. The lower 12 bits are the port number. This allows for bridges with up to 4095 ports. As a result, the bridge administrator can set the *Port priority* in steps of 4096, when viewed as a 16-bit number. The default value is **32768** (8000H), and the max. value is **61440** (F000H). When viewed as 4-bit number, the default value is **8** (8H), the min. value is **0** (0H), and the max. value is **15** (FH).

The following figure presets the *Port Identifier* (interpretation according to IEEE 802.1D-1998):



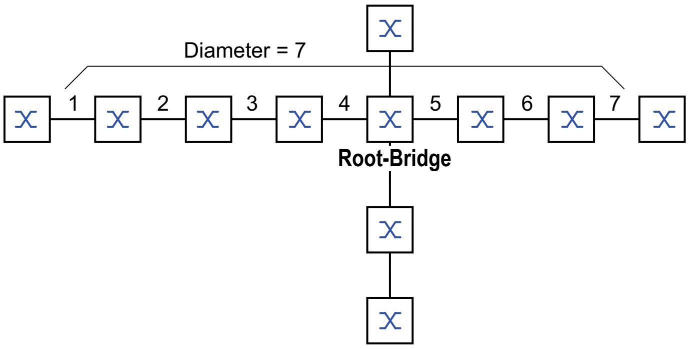
Max Age and Diameter

The “Max Age” and “Diameter” values largely determine the maximum expansion of a Spanning Tree network.

Diameter

The number of connections between the devices in the network that are furthest removed from each other is defined as the network diameter.

The following figure presents the definition of diameter:



The network diameter that can be achieved in the network is MaxAge-1.

In the state on delivery, `MaxAge = 20` and the maximum diameter that can be achieved is 19. When you set the maximum value of 40 for MaxAge, the maximum diameter that can be achieved is 39.

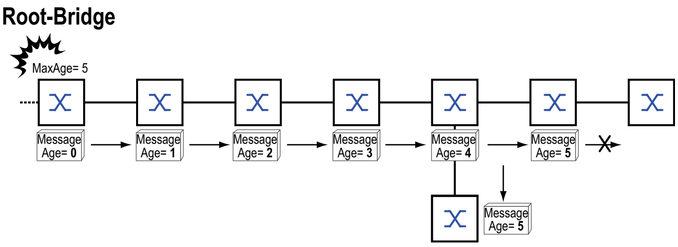
MaxAge

Every STP-BPDU contains a “MessageAge” counter. When a bridge is passed through, the counter increases by 1.

Before forwarding a STP-BPDU, the bridge compares the “MessageAge” counter with the “MaxAge” value specified in the device:

- When MessageAge < MaxAge, the bridge forwards the STP-BPDU to the next bridge.
- When MessageAge = MaxAge, the bridge discards the STP-BPDU.

The following figure presents the transmission of an STP-BPDU depending on MaxAge:



Rules for Creating the Tree Structure

Bridge Information

To determine the tree structure, the bridges need more detailed information about the other bridges located in the network.

To obtain this information, each bridge sends a BPDU (Bridge Protocol Data Unit) to the other bridges.

The contents of a BPDU include:

- *Bridge Identifier*
- *Root path cost*
- *Port Identifier*

(see IEEE 802.1D)

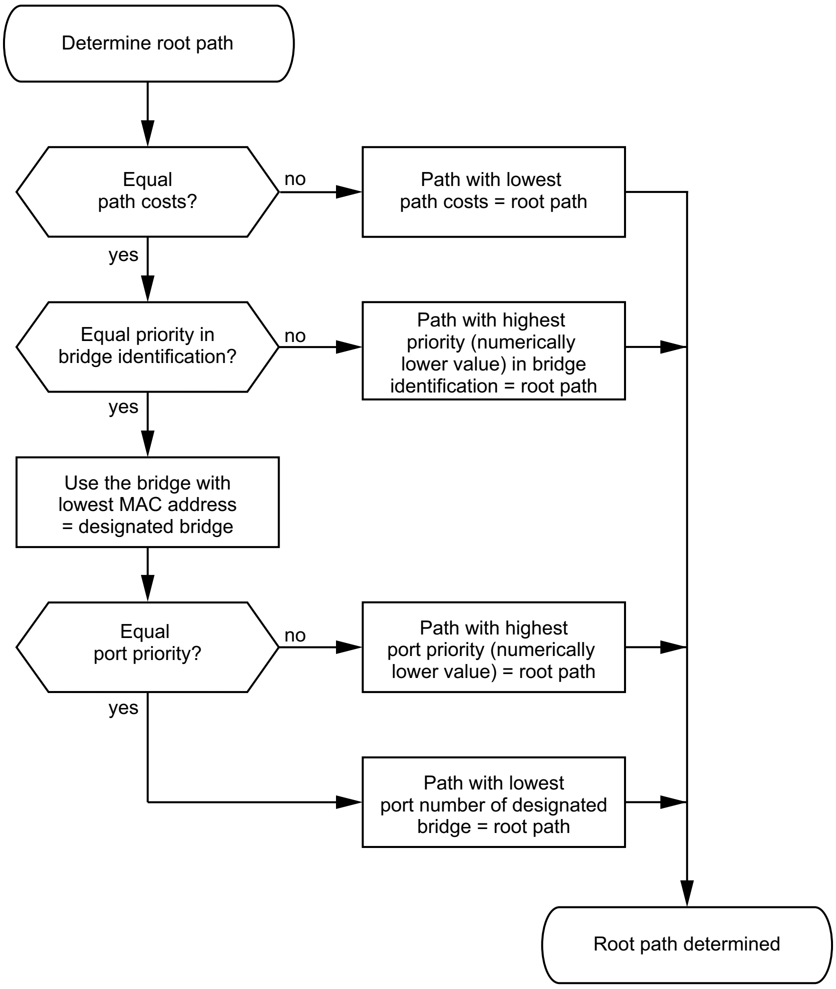
Setting Up the Tree Structure

The bridge with the numerically lowest *Bridge Identifier* value is called the *Root bridge*. This bridge is (or will become) the root of the tree structure.

The structure of the tree depends on the *root path cost*. Spanning Tree selects the structure so that the path costs between each individual bridge and the *Root bridge* become as small as possible.

- When there are multiple paths with the same *root path cost*, the bridge further away from the root determines which port it blocks. For this purpose, the bridge further from the root uses the *Bridge Identifiers* of the bridge closer to the root. The bridge further from the root blocks the port that leads to the bridge with the numerically greater ID. When 2 bridges have the same priority, the bridge with the numerically larger MAC address has the numerically ID, which is the option that is numerically larger and therefore less preferred when STP is comparing identifiers.
- When multiple paths with the same *root path cost* lead from one bridge to the same bridge, the bridge further away from the root uses the *Port Identifier* of the other bridge as the last criterion Port Identifier (interpretation according to IEEE 802.1D-1998). In the process, the bridge blocks the port that leads to the port with the numerically greater ID. A numerically greater ID is the option that is numerically larger and therefore less preferred when STP is comparing identifiers. When 2 ports have the same priority, the port with the greater port number has the numerically greater ID.

This flowchart presents the process for specifying the root path:


Determine root path
Equal path costs?
no
yes
Path with lowest path costs = root path
Equal priority in bridge identification?
no
yes
Path with highest priority (numerically lower value) in bridge identification = root path
Use the bridge with lowest MAC address = designated bridge
Equal port priority?
no
yes
Path with highest port priority (numerically lower value) = root path
Path with lowest port number of designated bridge = root path
Root path determined

Examples

Example of Determining the Root Path

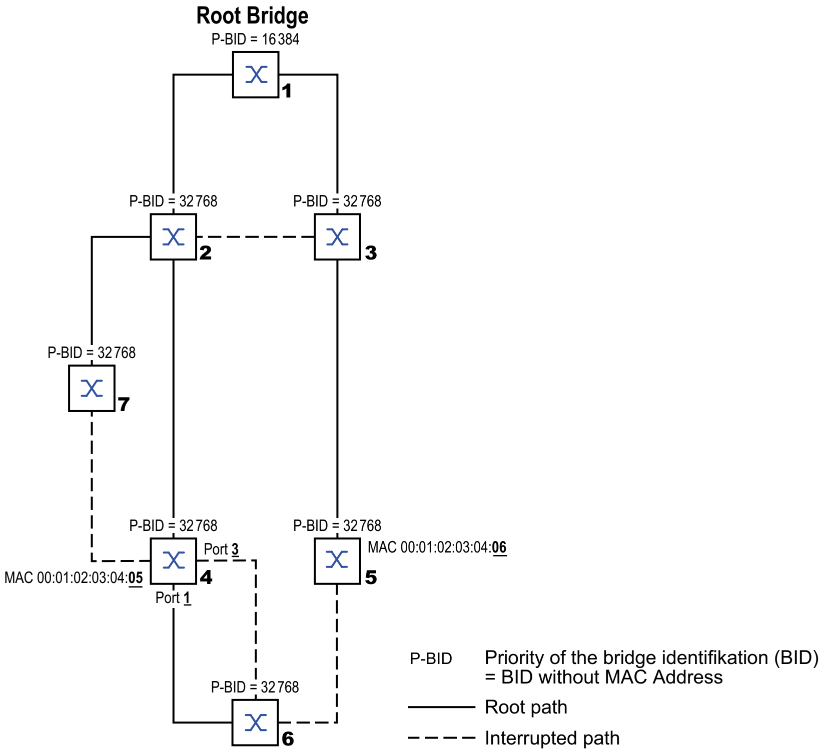
You can use the network plan to follow the flowchart for specifying the root path for determining the root path. The administrator has specified a priority in the *Bridge Identifier* for each bridge. The bridge with the numerically lowest value for the *Bridge Identifier* takes on the role of the *Root bridge*, in this case, bridge 1. In the example every sub-path has the same path costs. The protocol blocks the path between bridge 2 and bridge 3 because a connection from bridge 3 through bridge 2 to the *Root bridge* would result in greater path costs.

The path from bridge 6 to the *Root bridge* is interesting:

- The path through bridge 5 and bridge 3 has the same *root path cost* as the path through bridge 4 and bridge 2.
- STP selects the path using the bridge that has the lowest MAC address in the *Bridge Identifier* (bridge 4 in the illustration).
- There are also 2 paths between bridge 6 and bridge 4.

  The *Port Identifier* is decisive here (Port 1 < Port 3).

The following figure presents an example of a network plan for determining the root path:



NOTE: When the *Root bridge* goes down, the MAC address in the *Bridge Identifier* alone determines which bridge becomes the new *Root bridge*, because the administrator does not change the default values for the priorities of the bridges in the *Bridge Identifier*, apart from the value for the *Root bridge*.

Example of Manipulating the Root Path

You can use the network plan to follow the flowchart for specifying the root path. The administrator has performed the following actions:

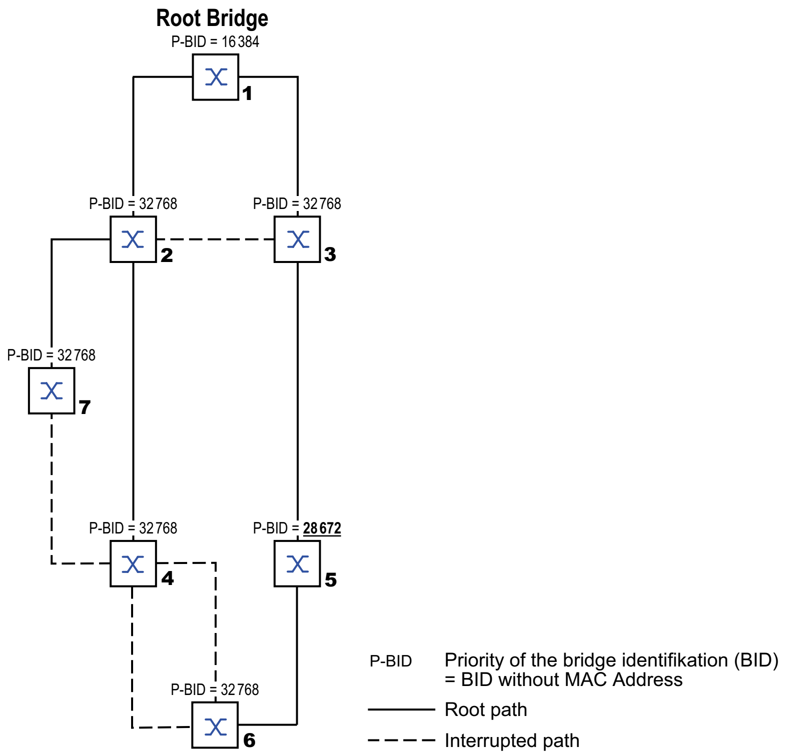
- Left the default value of 32768 (8000H) for every bridge apart from bridge 1 and bridge 5, and
- Assigned to bridge 1 the value 16384 (4000H), thus making it the *Root bridge*.
- Assigned the value 28672 (7000H) to bridge 5.

The protocol blocks the path between bridge 2 and bridge 3 because a connection from bridge 3 through bridge 2 to the *Root bridge* would result in greater path costs.

The path from bridge 6 to the *Root bridge* is interesting:

- The bridges select the path through bridge 5 because the value 28672 for the priority in the *Bridge Identifier* is lower than the value 32768.

The following figure presents an example of a network plan for manipulating the root path:

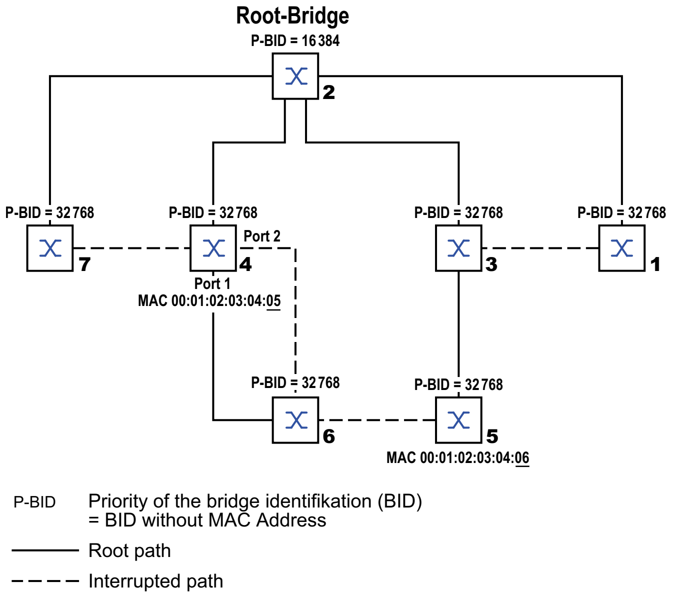


Example of Manipulating the Tree Structure

The administrator soon discovers that this configuration with bridge 1 as the *Root bridge* is invalid. On the paths from bridge 1 to bridge 2 and bridge 1 to bridge 3, the control packets which the *Root bridge* sends to every other bridge add up.

When the administrator sets up bridge 2 as the *Root bridge*, the burden of the control packets on the subnets is distributed much more evenly. The result is the configuration shown in the following figure. The path costs for most of the bridges to the *Root bridge* have decreased.

The following figure presents an example of manipulating the tree structure:



Rapid Spanning Tree Protocol

The Rapid Spanning Tree Protocol (RSTP) uses the same algorithm as Spanning Tree Protocol (STP) to determine the tree structure. However, when a link or bridge becomes inoperable, the Rapid Spanning Tree Protocol (RSTP) introduces mechanisms that accelerate the reconfiguration.

The ports play a significant role in this context.

Port Roles

Each bridge port in RSTP is assigned one of the following roles:

- *Root port*:

  The Root Port on a bridge is the port that provides the lowest-cost path to the *Root bridge*.

  When there are multiple ports with equally low path costs, the *Bridge Identifier* of the bridge that leads to the root (*Designated bridge*) determines which of its ports is given the role of the *Root port* by the bridge further away from the root.

  When a bridge has multiple ports with equally low path costs to the same bridge, the bridge uses the port ID of the bridge leading to the root (*Designated bridge*) to determine which port it selects locally as the *Root port*. Refer to the flowchart for specifying the root path.

  The *Root bridge* does not have a *Root port*, only *Designated ports*.

- *Designated port*:

  On each network segment, the bridge with the numerically lowest *root path cost* value to the Root Bridge becomes the *Designated bridge*.

  When more than one bridge has the same *root path cost*, the bridge with the numerically lowest *Bridge Identifier* value becomes the *Designated bridge*. The *Designated port* is the port on this bridge that connects a network segment leading away from the *Root bridge*. If a bridge connects to a network segment through more than one port (through a hub, for example), the port with the lowest Port ID is assigned as the *Designated Port*.

- *Edge port*

  An *Edge port* is a *Designated port* connected to an end device and not to another RSTP bridge. Because it does not exchange RST BPDUs, it does not affect the Spanning Tree topology and transitions immediately to the forwarding state.

- *Alternate port*

  A port that provides an alternate path to the *Root bridge*. It remains in the discarding state and becomes the *Root port* if the current *Root Port* is no longer available.

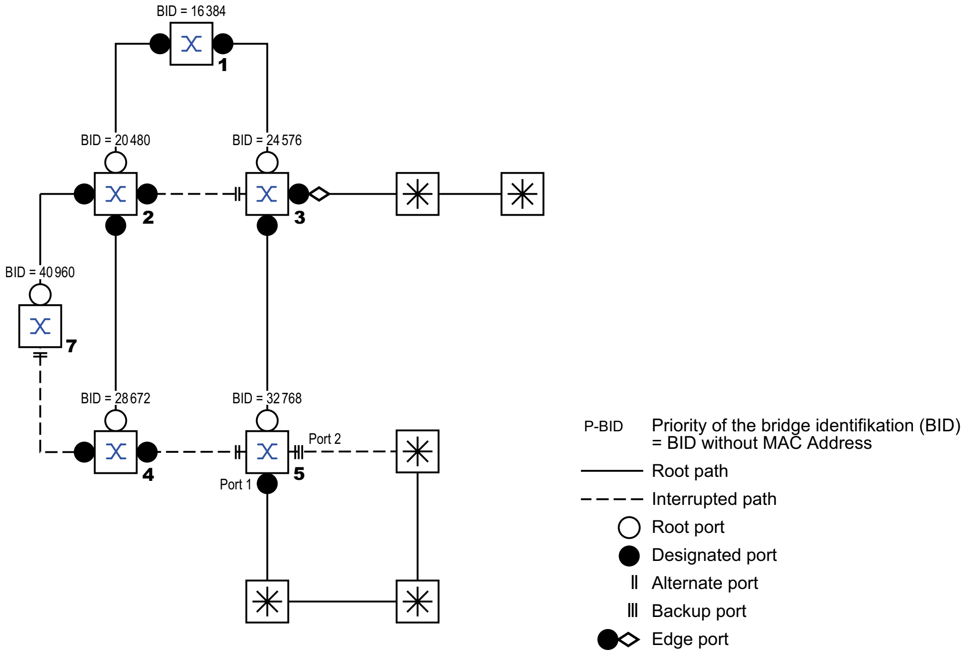
- *Backup port*

  This is a blocked port that serves as a backup in case the connection to the *Designated port* of this network segment (without any RSTP bridges) is lost

- Disabled port

  This port does not participate in the Spanning Tree Operation. It is either administratively disabled or physically disconnected.

This flowchart presents the process for the port role assignment:



Port States

Depending on the tree structure and the state of the selected connection paths, RSTP assigns the ports their states.

The following table describes the relationship between port state values for STP and RSTP:

STP port state	Administrative bridge port state	MAC Operational	RSTP port state	Active topology (port role)
Disabled	Disabled	FALSE	*Discarding*[1]	Excluded (disabled)
Disabled	Enabled	FALSE	*Discarding*[a]	Excluded (disabled)
Blocking	Enabled	TRUE	*Discarding*[2]	Excluded (alternate, backup)
Listening	Enabled	TRUE	*Discarding*[b]	Included (root, designated)
Learning	Enabled	TRUE	*Learning*	Included (root, designated)
Forwarding	Enabled	TRUE	*Forwarding*	Included (root, designated)

[1] The dot1d-MIB displays *Disabled*.

[2] The dot1d-MIB displays *Blocked*.

Meaning of the RSTP port states:

- *Disabled*: Port does not belong to the active topology
- *Discarding*: No address learning in the MAC address table (forwarding database), no data packets except for STP-BPDUs
- *Learning*: Address learning active in the MAC address table (forwarding database), no data packets apart from STP-BPDUs
- *Forwarding*: Address learning in the MAC address table (forwarding database) active, sending and receiving of every packet type (not only STP-BPDUs)

Spanning Tree Priority Vector

To assign roles to the ports, the RSTP bridges exchange configuration information with each other. This information is defined as the Spanning Tree Priority Vector. It is part of the *RST BPDUs* and contains the following information:

- *Bridge Identifier* of the *Root bridge*
- *root path cost* of the sending bridge
- *Bridge Identifier* of the sending bridge
- *Port Identifier* of the port through which the message was sent
- *Port Identifier* of the port through which the message was received

Based on this information, the bridges participating in RSTP are able to determine port roles themselves and define the port states of their own ports.

Fast Reconfiguration

The RSTP reacts faster than STP to an interruption of the root path in the following situations:

- Introduction of edge-ports:

  During a reconfiguration, RSTP sets an *Edge port* into the transmission mode after 3 seconds (default setting). To ascertain that no bridge sending BPDUs is connected, RSTP waits for the “Hello Time” to elapse.

  When you verify that an end device is and remains connected to this port, there are no waiting times at this port in the case of a reconfiguration.
- Introduction of *Alternate ports*:

  As the port roles are already distributed in normal operation, a bridge can immediately switch from the *Root port* to the *Alternate port* after the connection to the *Root bridge* is lost.
- Communication with neighboring bridges (point-to-point connections):

  Decentralized, direct communication between neighboring bridges enables reaction without wait periods to status changes in the spanning tree topology.
- Address table:

  With Spanning Tree Protocol (STP), the age of the entries in the MAC address table (forwarding database) determines the updating of communication. The Rapid Spanning Tree Protocol (RSTP) immediately deletes the entries in those ports affected by a reconfiguration.
- Reaction to events:

  Without having to match any time specifications, Rapid Spanning Tree Protocol (RSTP) immediately reacts to events, for example, connection interruption and connection reinstatement.

NOTE: Data packages could be duplicated and/or arrive in an incorrect order at the recipient during the reconfiguration phase of the RSTP topology. You may also use the Spanning Tree Protocol (STP) or select another redundancy procedure described in this manual.

Configuring the Device

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Spanning Tree configuration individually.
- Complete the configuration of the other devices of the Spanning Tree configuration before you connect the redundant lines.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

RSTP sets up the network topology completely autonomously. The device with the numerically lowest *Bridge priority* value automatically becomes the *Root bridge*. However, to define a specific network structure, you specify a device as the *Root bridge*. In general, a device in the backbone takes on this role.

Perform the following steps:

Step	Action
1	Set up the network to meet your requirements, initially without redundant lines.
2	Deactivate the flow control on the participating ports. If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended. Default setting: The flow control is deactivated globally and it is activated on every port.
3	Disable MRP on every device.
4	Enable Spanning Tree on every device in the network. In the state on delivery, Spanning Tree is switched on in the device.
5	Navigate to **Switching** > **L2-Redundancy** > **Spanning Tree** > **Global**.
6	Enable the function.
7	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`spanning-tree operation`	To enable Spanning Tree.
`show spanning-tree global`	To display the parameters for verifying.

Now connect the redundant lines and define the settings for the device that takes over the role of the *Root bridge*. To do this, perform the following steps:

Step	Action
1	In the **Priority** field you specify a numerically lower value. The bridge with the numerically lowest *Bridge Identifier* value has the highest priority and becomes the *Root bridge* of the network.
2	To apply the settings, click the ✓ button.
3	To specify the *Bridge priority* of the device, execute the following command: `spanning-tree mst priority 0 <0..61440>` **NOTE:** Specify the *Bridge priority* in the range `0..61440` in steps of 4096.
4	After saving, the dialog shows the following information: • The **Bridge is root** checkbox is selected. • The **Root port** field shows the value **0.0**. • The **Root path cost** field shows the value **0**.
5	To display the parameters for verifying, execute the following command: `show spanning-tree global`
6	If applicable, change the values in the **Forward delay [s]** and **Max age** fields. The *Root bridge* transmits the changed values to the other devices.
6	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`spanning-tree forward-time <4..30>`	To specify the delay time for the status change in seconds.
`spanning-tree max-age <6..40>`	To specify the maximum permissible branch length, for example the number of devices to the *Root bridge*.
`show spanning-tree global`	To display the parameters for verifying.

NOTE: The parameters Forward delay [s] and Max age have the following relationship:

- Forward delay [s] ≥ (Max age/2) + 1.
- If you enter values in the fields that contradict this relationship, the device replaces these values with the last valid values or with the default value.

NOTE: Whenever possible, leave the **Hello Time** field as the default value.

Verify the following values in the other devices:

- *Bridge Identifier* (*Bridge priority* and MAC address) of the corresponding device and the *Root bridge*.
- Number of the port that leads to the *Root bridge*.
- Path cost from the *Root port* of the device to the *Root bridge*.

Execute the following command:

Command	Description
`show spanning-tree global`	To display the parameters for verifying.

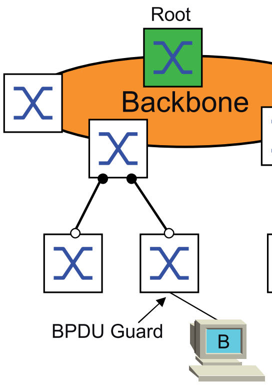
Guards

The device allows the activation of various protection functions (guards) on the ports.

The following protection functions help protect the network from incorrect configurations, loops and attacks with STP-BPDUs:

- BPDU guard – for manually specified *Edge ports* (ports connected to an end device)

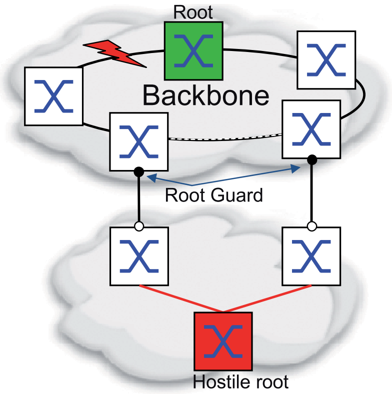
  You activate this protection function globally in the device.

  Ports connected to an end device do not normally receive any STP-BPDUs. If an attacker attempts to feed in STP-BPDUs on this port, the device deactivates the port.

- Root guard – for *Designated ports*

  You activate this protection function separately for every port.

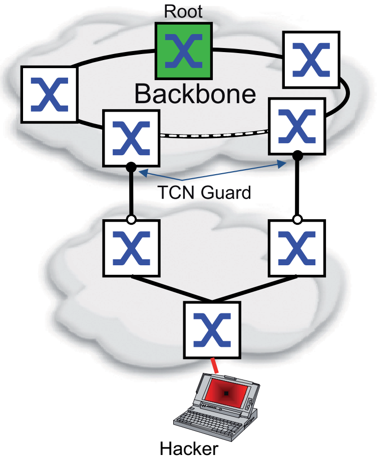
  

  When a *Designated port* receives an STP-BPDU with better path information to the *Root bridge*, the device discards the STP-BPDU and sets the transmission state of the port to **discarding** instead of **root**.

  When there are no STP-BPDUs with better path information to the *Root bridge*, after 2 × Hello time [s] the device resets the state of the port to a value according to the port role.

- TCN guard – for ports that receive STP-BPDUs with a *Topology Change* flag

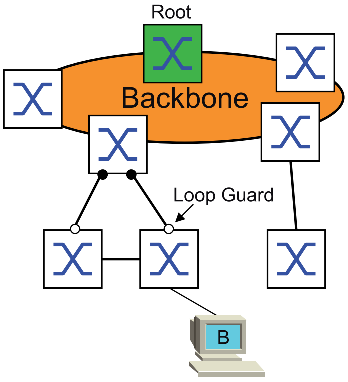
  You activate this protection function separately for every port.



  If the protection function is activated, the device ignores *Topology Change* flags in received STP-BPDUs. This does not change the content of the MAC address table (forwarding database) of the port. However, additional information in the BPDU that changes the topology is processed by the device.

- Loop guard – for *Root ports*, *Alternate ports* and *Backup ports*

  You activate this protection function separately for every port.



  If the port does not receive any more STP-BPDUs, this protection function helps prevent the transmission status of a port from unintentionally being changed to **forwarding**. If this situation occurs, the device designates the loop status of the port as inconsistent, but does not forward any data packets.

Activating the BPDU Guard Function

Perform the following steps:

Step	Action
1	Navigate to **Switching > L2-Redundancy > Spanning Tree > Global**.
2	Select the BPDU guard checkbox.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`spanning-tree bpdu-guard`	To activate the BPDU guard function.
`show spanning-tree global`	To display the parameters for verifying.

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **L2-Redundancy** > **Spanning Tree** > **Port**.
2	Switch to the **CIST** tab.
3	For the ports connected to an end device, select the checkbox in the Admin edge port column.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`interface <x/y>`	To change to the Interface Configuration mode of interface <x/y>.
`spanning-tree edge-port`	To designate the port as *an Edge port* (port connected to an end device).
`show spanning-tree port x/y`	To display the parameters for verifying.
`exit`	To leave the interface mode.

When an *Edge port* receives an STP-BPDU, the device behaves as follows:

- The device deactivates this port.

  In the **Basic Settings > Port** dialog, **Configuration** tab, the checkbox for this port in the Port on column is cleared.
- The device designates the port.

You can determine if a port has disabled itself because of a received BPDU. To do this, perform the following steps:

Step	Action
1	In the **Switching** > **L2-Redundancy** > **Spanning Tree** > **Port**, **Guards** tab, select the checkbox in the BPDU guard effect column.
2	To display the parameters of the port for verifying, execute the following command: `show spanning-tree port x/y` The value of the BPDU guard effect parameter is **enabled**.

Reset the status of the port to the value **forwarding**. To do this, perform the following steps:

Step	Action
1	When the port still receives BPDUs: • Remove the manual definition as an *Edge port* (port connected to an end device). or • Deactivate the BPDU guard function.
2	Activate the port again.

Activating the Root Guard / TCN Guard / Loop Guard Function

Perform the following steps:

Step	Action
1	Navigate to **Switching > L2-Redundancy > Spanning Tree > Port**.
2	Switch to the **Guards** tab.
3	For *Designated ports*, select the checkbox in the Root guard column.
4	For ports that receive STP-BPDUs with a *Topology Change* flag, select the checkbox in the TCN guard column.
5	For *Root ports*, *Alternate ports* or *Backup ports*, select the checkbox in the Loop guard column. **NOTE:** The Root guard and Loop guard functions are mutually exclusive. If you try to activate the Root guard function while the Loop guard function is active, the device deactivates the Loop guard function.
6	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface <x/y>`	To change to the Interface Configuration mode of interface **<x/y>**.
`spanning-tree guard-root`	To activate the Root guard function on the *Designated port*.
`spanning-tree guard-tcn`	To activate the TCN guard function on the port that receives STP-BPDUs with a *Topology Change* flag.
`spanning-tree guard-loop`	To activate the Loop guard function on a *Root port*, *Alternate port*, or *Backup port*.
`exit`	To leave the interface mode.
`show spanning-tree port x/y`	To display the parameters of the port for verifying.

Link Aggregation

The Link Aggregation function using the single switch method helps you overcome 2 limitations with Ethernet links, namely bandwidth, and redundancy.

The Link Aggregation function helps you overcome bandwidth limitations of individual ports. The Link Aggregation function allows two or more connections into one logical connection between 2 devices. The parallel links increase the bandwidth between the 2 devices.

You typically use the Link Aggregation function on the network backbone. The function provides you an inexpensive way to incrementally increase bandwidth.

Furthermore, the Link Aggregation function provides for redundancy with a seamless switchover. When a link goes down, with 2 or more links set up in parallel, the other links in the group continue to forward the data packets.

The device uses a hash option to determine load balancing across the port group. Tagging the egress data packets allows transmission of associated packets across the same link.

The default settings for a new Link Aggregation instance are as follows:

- In the Configuration frame, the value in the **Hashing option** field is **sourceDestMacVlan**.
- In the Active column, the checkbox is selected.
- In the Send trap (Link up/down) column, the checkbox is selected.
- In the Static link aggregation column, the checkbox is cleared.
- In the Hashing option column, the value is **sourceDestMacVlan**.
- In the Active ports (min.) column, the value is **1**.

Methods of Operation

The device operates on the Single Switch method. The Single Switch method provides you an inexpensive way to grow the network. The single switch method states that you need one device on each side of a link to provide the physical ports. The device balances the network load across the group member ports.

The device also uses the Same Link Speed method in which the group member ports operate in full-duplex, point-to-point links having the same transmission rate. The first port that you add to the group is the primary port and determines the bandwidth for the other member ports of the Link Aggregation Group.

The device allows set a maximum of 2 Link Aggregation groups.

Hash Algorithm

The frame distributor receives frames from the end devices and transmitting them over the Link Aggregation Group. The frame distributor implements a distribution algorithm used for choosing the link for transmitting any given packet. The hash option helps you achieve load balancing across the group.

The following list contains options which you set for link selection.

- Source MAC address, VLAN ID, EtherType, and receiving port
- Destination MAC address, VLAN ID, EtherType, and receiving port
- Source/Destination MAC address, VLAN ID, EtherType, and receiving port
- Source IP address and Source TCP/UDP port
- Destination IP address and destination TCP/UDP port
- Source/destination IP address and source/destination TCP/UDP port

Static and Dynamic Links

The device allows static and dynamic links.

- Static Links

  The administrator sets up and maintains the links manually. For example, when a link is interrupted and there is a media converter between the devices, the media converter continues forwarding the data packets on the link, causing the link to be interrupted. Another possibility is that cabling or an undetected configuration error causes undesirable network behavior. In this case, the network administrator manually changes the link setup to restore the data stream.
- Dynamic Links

  The device confirms that the setup on the remote device can handle link aggregation and switchover occurs automatically.

Link Aggregation Example

Loops during the configuration phase may lead to unintended equipment operation.

⚠ WARNING

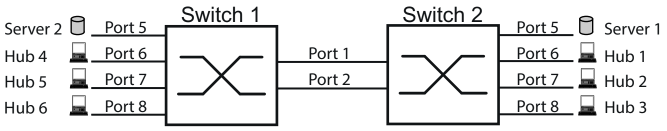
UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Link Aggregation configuration individually.
- Complete the configuration of the other devices of the Link Aggregation configuration before you connect the redundant lines.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Connect multiple workstations using one aggregated link group between Switch 1 and Switch 2. By aggregating multiple links, greater speeds are achievable without a hardware upgrade.

The following figure presents a Link Aggregation switch to switch network:



Set up Switch 1 and 2 in the Graphical User Interface. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching > L2-Redundancy > Link Aggregation**.
2	Click the + button. The dialog displays the Create window.
3	From the Trunk port drop-down list, select the instance number of the link aggregation group.
4	From the Port drop-down list, select port ***1/1***.
5	Click **OK**.
6	Repeat the preceding steps and select the port ***1/2***.
7	Click **OK**.
8	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`link-aggregation add lag/1`	To add a Link Aggregation Group **lag/1**.
`link-aggregation modify lag/1 addport 1/1`	To add port ***1/1*** to the Link Aggregation Group.
`link-aggregation modify lag/1 addport 1/2`	To add port ***1/2*** to the Link Aggregation Group.

Link Backup

Link Backup provides a redundant link for the data packets on Layer 2 devices. When the device detects an error on the primary link, the device transfers the data packets to the backup link. You typically use Link Backup in service-provider or enterprise networks.

You set up the backup links in pairs, one as a primary and one as a backup. When providing redundancy for enterprise networks for example, the device lets you set up more than one pair. The maximum number of link backup pairs is: `total number of physical ports / 2`. Furthermore, when the state of a port participating in a link backup pair changes, the device sends an SNMP trap.

When configuring link backup pairs, remember the following rules:

- A link pair consists of any combination of physical ports. For example, one port is a 100 Mbit port and the other is a 1000 Mbit SFP port.
- A specific port is a member of one link backup pair at any given time.
- Verify that the ports of a link backup pair are members of the same VLAN with the same VLAN ID. When the *Primary port* or *Backup port* is a member of a VLAN, assign the second port of the pair to the same VLAN.

The default setting for this function is inactive without any link backup pairs.

NOTE: Verify that the Spanning Tree Protocol (STP) is disabled on the Link Backup ports.

`Fail Back` Description

Link Backup also allows a `Fail Back` option. When you activate the `Fail Back` function and the *Primary port* returns to normal operation, the device first blocks the data packets on the *Backup port* and then forwards the data packets to the *Primary port*. This process helps protect the device from causing loops in the network.

When the *Primary port* returns to the link up and active state, the device supports 2 modes of operation:

- When you inactivate `Fail Back`, the *Primary port* remains in the **blocking** state until the backup link is interrupted.
- When you activate `Fail Back`, and after the `Fail Back` delay [s] timer expires, the *Primary port* returns to the **forwarding** state and the *Backup port* changes to down.

In the cases previously listed, the port forcing its link to forward the data packets, first sends a *Topology Change* packet to the remote device. The *Topology Change* packet helps the remote device rediscover the MAC addresses.

Application example for the Link Backup function

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Link Backup configuration individually.
- Complete the configuration of the other devices of the Link Backup configuration before you connect the redundant lines.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

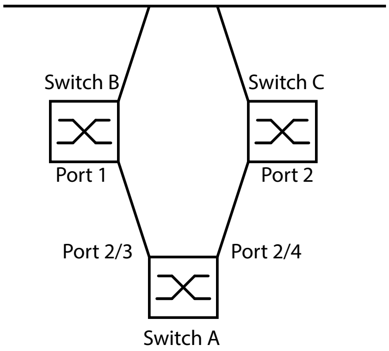
In the following example network, you connect ports ***2/3*** and ***2/4*** on Switch A to the uplink Switches B and C. When you set up the ports as a Link Backup pair, one of the ports forwards the data packets and the other port is in the *blocking* state.

The *Primary port* ***2/3*** on Switch A, is the active port and is forwarding the data packets to port 1 on Switch B. Port ***2/4*** on Switch A is the *Backup port* and blocks the data packets.

When Switch A disables port ***2/3*** because of a detected error, port ***2/4*** on Switch A starts forwarding data packets to port 2 on Switch C.

When port ***2/3*** returns to the active state, “no shutdown“, with `Fail Back` activated, and `Fail Back` delay [s] set to 30 seconds. After the timer expires, port ***2/4*** first blocks the data packets and then port ***2/3*** starts forwarding data packets.

The following figure presents the Link Backup example network



The following tables contain examples of parameters to set up Switch A.

Perform the following steps:

Step	Action
1	Navigate to **Switching > L2-Redundancy > Link Backup**.
2	Enter a new Link Backup pair in the table: • Click the ⊞ button. The dialog displays the Create window. • From the Primary port drop-down list, select port ***2/3***. From the Backup port drop-down list, select port ***2/4***. • Click **OK**.
3	In the Description textbox, enter **Link_Backup_1** as the name for the backup pair.
4	To activate the `Fail Back` function for the link backup pair, select the `Fail Back` checkbox.
5	Set the `Fail Back` timer for the link backup pair, enter **30** s in `Fail Back` delay [s].
6	To activate the link backup pair, select the Active checkbox.
7	Enable the Link Backup function. Select the **On** radio button in the Operation frame.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 2/3`	To change to the Interface Configuration mode of interface ***2/3***.
`link-backup add 2/4`	To add a Link Backup instance where port ***2/3*** is the *Primary port* and port ***2/4*** is the *Backup port*.
`link-backup modify 2/4 description Link_Backup_1`	To specify the string **Link_Backup_1** as the name of the backup pair.
`link-backup modify 2/4 failback-status enable`	To enable the `Fail Back` delay.
`link-backup modify 2/4 failback-time 30`	To specify the time for the `Fail Back` delay as **30** s.
`link-backup modify 2/4 status enable`	To enable the Link Backup instance.
`exit`	To change to the Configuration mode.
`link-backup operation`	To enable the Link Backup function globally in the device.

FuseNet Function

The FuseNet protocols let you couple rings that are operating with one of the following redundancy protocols:

- MRP
- HIPER Ring
- RSTP

NOTE: The prerequisite for coupling a network to the main ring using the Ring/Network Coupling function is that the connected network contains only network devices that support the Ring/Network Coupling function.

Use the following table to select the FuseNet coupling protocol to be used in the network:

Main Ring	**Connected Network**		
	MRP	**HIPER Ring**	**RSTP**
MRP	Sub Ring(1)	– RCP – Ring/Network Coupling	– RCP – Ring/Network Coupling
HIPER Ring	Sub Ring	Ring/Network Coupling	– RCP – Ring/Network Coupling
RSTP	RCP	RCP	–

(1) With the MRP function set-up on different VLANs.

– No suitable coupling protocol.

Sub Ring

The Sub Ring function allows a Sub Ring to couple a main ring that can use various protocols. The Sub Ring protocol provides redundancy for devices by coupling both ends of an otherwise flat network to a main ring.

The prerequisite is that main ring operates with the one of the following redundancy protocols:

- MRP
- RSTP
- HIPER Ring

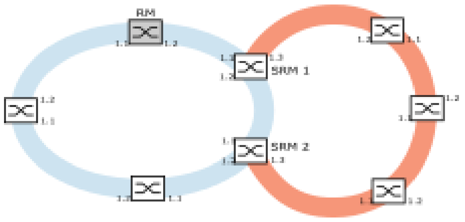
Setting up Sub Rings has the following advantages:

- Through the coupling process, you include the new network segment in the redundancy concept.
- You can integrate new areas into existing networks.
- You can map the organizational structure of an area in a network topology.
- In a Sub Ring coupled to an MRP Ring, the switchover times of the Sub Ring in redundancy cases are typically <100 ms.

Sub Ring Description

The Sub Ring concept allows new network segments couple with suitable devices in an existing ring (main ring). The devices with which you couple the Sub Ring to the main ring are Sub Ring Managers (SRM).

The following figure presents an example of a Sub Ring structure:



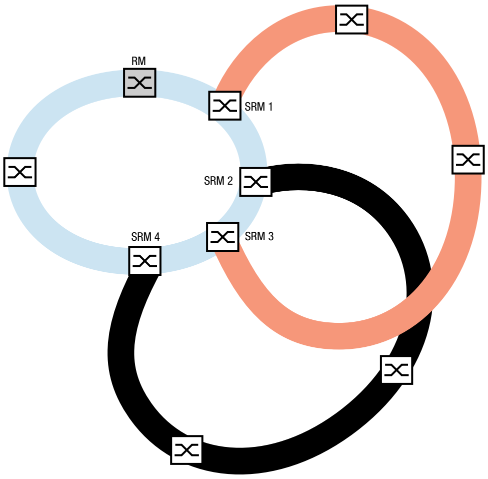
Blue ring: Main ring
Orange ring: Sub Ring
SRM: Sub Ring Manager
RM: Ring Manager

The *Sub Ring Manager* capable devices support up to 8 instances and thus manage up to 8 Sub Rings at the same time.

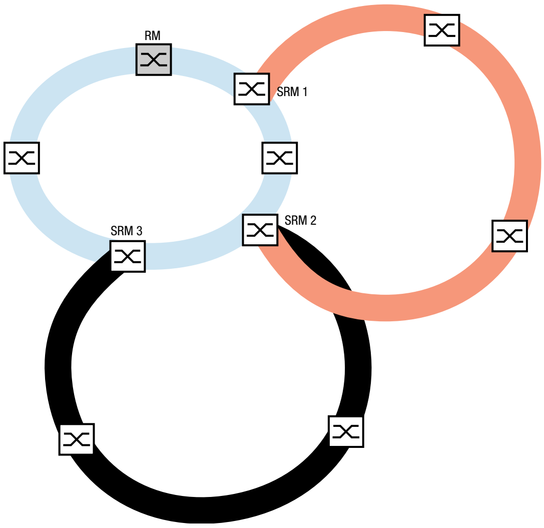
The Sub Ring function allows devices that support MRP as participants. The devices with which you couple the Sub Ring to the main ring require the Sub Ring Manager function.

Each Sub Ring can consist of up to 200 participants, in addition to the *Sub Ring Manager* devices themselves and the devices between the *Sub Ring Manager* devices in the main ring.

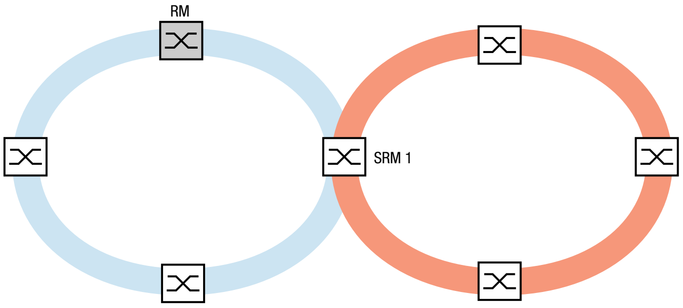
The following figure presents an example of an overlapping Sub Ring structure:



The following figure presents a Special case: A *Sub Ring Manager* device manages 2 Sub Rings (2 instances). The *Sub Ring Manager* device is capable of managing up to 8 instances:



The following figure presents a Special case: A *Sub Ring Manager* device manages both ends of a Sub Ring on different ports (*Single Sub Ring Manager*):



If you use MRP for the main ring, specify the VLAN settings as follows:

- VLAN **X** for the main ring:
  - On the ring ports of the main ring participants
  - On the main ring ports of the *Sub Ring Manager* device
- VLAN **Y** for the Sub Ring (another VLAN ID than VLAN **X**):
  - On the ring ports of the devices participating in the Sub Ring
  - On the Sub Ring ports of the *Sub Ring Manager* device

  You can use the same VLAN for multiple Sub Rings.

Advanced Information

Sub Ring Packets

The Sub Ring protocol uses *Test*, *Link Change*, and *Topology Change* (*FDB Flush*) packets.

The 2 SRMs connect the Sub Ring with one Sub Ring port each. The SRMs have different roles, **manager** and **redundantManager**. In case of only one SRM, this SRM has 2 Sub Ring ports. The SRM has the role **singleManager** and takes on the functions of both SRMs in the normal configuration.

As long as the connections in the Sub Ring are operational, the SRM with the role **redundantManager** sets its Sub Ring port into the *blocking* state. In this state, this Sub Ring port receives and sends only Sub Ring packets, it neither receives nor sends normal (payload) data packets. This way, this SRM helps prevent a network loop in the Sub Ring.

Both SRMs periodically send test packets into the Sub Ring. The test packets are special packets. The SRMs expect to receive the test packets of their partner SRM. The SRM with the role **redundantManager** sends and receives test packets even at its redundant Sub Ring port although the redundant Sub Ring port blocks normal (payload) packets.

If the SRM with the role **redundantManager** does not receive test packets for a specified time, the SRM detects a Sub Ring interruption. The SRM then unblocks its redundant Sub Ring port. Conversely, if the SRM again receives test packets from its partner SRM, the SRM sets its redundant port into *blocking*.

On reconfiguration of the Sub Ring, the SRM also flushes its MAC address table (forwarding database) and sends *Topology Change* packets to the Sub Ring participants. The *Topology Change* packets also prompt the devices participating in the Sub Ring to flush their MAC address table (forwarding database). This procedure helps forward the payload packets over the new path. This procedure applies regardless of whether the Sub Ring reconfiguration was caused by a *Link Down* or a *Link Up* notification.

The following table presents Sub Ring packets:

Packet Type	Send Mode	Time Parameter	Value
Test packet	Periodically	Send interval	40 ms[1]
		Reception timeout	280 ms[2]
Link Down packet[3]	Event-driven	On link-down of a Sub Ring port	–
Topology Change packet[4]	Event-driven	On Sub Ring reconfiguration	–

[1] For Sub Ring recovery time 100 ms.

[2] The maximum Sub Ring recovery time is 300 ms.

[3] Sent by supporting Sub Ring participants.

[4] The reception of a *Topology Change* packet prompts the supporting devices participating in the Sub Ring to flush their MAC address table (forwarding database).

Sub Ring Packet Prioritization

The devices participating in the Sub Ring send the test packets, the *Link Change* packets, and the *Topology Change* packets with a user-configurable VLAN ID. The default VLAN ID is 0. The devices send the test packets untagged and thus without priority (Class of Service) information.

To help minimize the reconfiguration time under high network load, you can add a VLAN tag and thus priority information to these packets. The devices then forward and send these packets with the IEEE 802.1Q Class of Service priority 7 (Network control).

To prioritize the test packets, perform the following steps on every device in the Sub Ring:

- Specify the VLAN ID for the Sub Ring test packets to a value ≥**1**.
- Specify the Sub Ring ports as **T** (tagged) members of this VLAN.

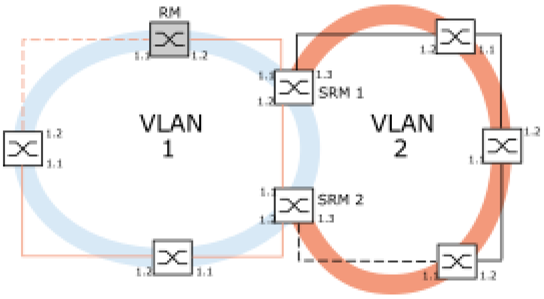
  NOTE: When you set the VLAN ID for the Sub Ring packets to a value ≥**1** in the **Switching > L2-Redundancy > FuseNet > Sub Ring** dialog, the device adds its Sub Ring ports as **T** (tagged) members of this VLAN. If the VLAN does not yet exist, the device automatically sets up this VLAN. After setting a new VLAN ID for the Sub Ring packets, verify the **Switching > VLAN > Configuration** dialog for the VLAN and the Sub Ring port membership settings.

Sub Ring Example

In the following example, you couple a new network segment with 3 devices to an existing main ring which uses the Media Redundancy Protocol (MRP). When you couple the network at both ends instead of one end, the Sub Ring provides increased availability with the corresponding configuration.

You couple the new network segment as a Sub Ring. You couple the Sub Ring to the existing devices of the main ring using the following configuration types.

The following figure presents an example of a Sub Ring structure with VLANs:



Orange line: Main ring members in VLAN 1
Black line: Sub Ring members in VLAN 2
Orange dashed line: Main ring loop open
Black dashed line: Sub Ring loop open
SRM: Sub Ring Manager
RM: Ring Manager

To set up the Sub Ring, set up the 3 devices of the new network segment as participants in an MRP Ring:

- To minimize the ring recovery time in case of a link-up after an interruption, set up the speed and duplex mode of the ring ports as follows:
  - For 100 Mbit/s TX ports, disable Automatic Negotiation and manually set up 100M FDX.
  - For the other port types, keep the port-specific default settings.

The following steps contain additional settings for Sub Ring configuration:

Step	Description
1	To help prevent loops during configuration, deactivate the Sub Ring function on the devices participating in the main ring and Sub Ring. After you completely set up every device participating in the main ring and Sub Rings, activate the global Sub Ring function in the *Sub Ring Manager* devices.
2	Disable the RSTP function on the MRP Ring ports used in the Sub Ring.
3	Verify that the Link Aggregation function is inactive on ports participating in the main ring and Sub Ring.
4	To minimize the ring recovery time in case of a link-up after an interruption, set up the speed and duplex mode of the Sub Ring ports as follows: • For 100 Mbit/s TX ports, disable Automatic Negotiation and manually set up 100M FDX. • For the other port types, keep the port-specific default settings.
5	Specify a different VLAN membership for the main ring ports and Sub Ring ports although the main ring is using the Media Redundancy Protocol (MRP). For example, use VLAN ID **1** for the main ring and the redundant link, then use VLAN ID **2** for the Sub Ring. • For the devices participating in the main ring for example, navigate to **Switching > VLAN > Configuration** dialog. Add VLAN **1** in the static VLAN table. To tag the main ring ports for membership in VLAN **1**, select **T** from the drop-down list of the appropriate port columns. • For the devices participating in the Sub Ring use the preceding step and add the ports to VLAN **2** in the static VLAN table.
6	Activate the MRP function for the devices participating in the main ring and Sub Ring. • In the **Switching > L2-Redundancy > MRP** dialog, select the 2 ports participating in the main ring on the devices participating in the main ring. • For the devices participating in the Sub Ring use the preceding steps and set up the 2 ports participating in the Sub Ring. • Assign the same MRP domain ID to the devices participating in the main ring and Sub Ring. When you only use Schneider Electric devices, the default values suffice for the MRP domain ID.

NOTE: The MRP domain is a sequence of 16 numbers in the range of **0** to **255**. The default value is **2255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255**. An MRP domain ID consisting entirely of zeros is invalid.

The **Switching > L2-Redundancy > FuseNet > Sub Ring** dialog allows a change of the MRP domain ID. As an alternative, you can use the Command Line Interface. To do this, execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain delete`	To delete the MRP domain.
`mrp domain add domain-id 0.0.1.1.2.2.3.4.4.111. 222.123.0.0.66.99`	To add an MRP domain with the specified MRP domain ID. Any subsequent MRP domain changes apply to this domain ID.

Application Example for the Sub Ring Function

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Sub Ring configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Set up the two *Sub Ring Manager* devices in the example. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching > L2-Redundancy > FuseNet > Sub Ring**.
2	To add a table row, click the ⊞ button.
3	In the Port column, select the port that couples the device to the Sub Ring. Use port ***1/3*** for this example. For coupling, use one of the available ports with the exception of the ports which are already connected to the main ring.
4	In the **Name** column, assign a name to the Sub Ring. For this example enter **Test**.
5	In the Administrative mode column, select the *Sub Ring Manager* mode. You thus specify which port for coupling the Sub Ring to the main ring becomes the redundant port of the *Sub Ring Manager* device. The options for the coupling are: • **manager** When you specify both *Sub Ring Manager* devices with the same value, the device with the greater MAC address manages the redundant link. • **redundant manager** This device manages the redundant link, as long as the other *Sub Ring Manager* device operates in the **manager** mode. Otherwise the device with the greater MAC address manages the redundant link. Specify for *Sub Ring Manager* device 1 the value **manager**, in accordance with the figure depicting this example.
6	Leave the values in the VLAN column and MRP domain column unchanged. The default values are correct for the example configuration.
7	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sub-ring add 1`	To add a Sub Ring with the Sub Ring ID **1**.
`sub-ring modify 1 port 1/3`	To specify port ***1/3*** as the Sub Ring port.
`sub-ring modify 1 name Test`	To assign the name **Test** to the Sub Ring **1**.
`sub-ring modify 1 mode manager`	To assign the **manager** mode to the Sub Ring **1**.
`show sub-ring ring`	To display the Sub Rings state on this device.
`show sub-ring global`	To display the Sub Ring global state on this device.

Set up the second *Sub Ring Manager* device in the same way.

Specify for *Sub Ring Manager* device 2 the value **redundant manager**, in accordance with the figure depicting this example.

Perform the following steps:

Step	Action
1	To activate the *Sub Ring Manager* mode, select the Active checkbox in the corresponding table row.
2	After you have set up both *Sub Ring Manager* devices and the devices participating in the Sub Ring, enable the function and close the redundant link.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sub-ring enable 1`	To activate Sub Ring **1**.
`sub-ring enable 2`	To activate Sub Ring **2**.
`exit`	To change to the Privileged EXEC mode.
`show sub-ring ring <Domain ID>`	To display the settings of the selected Sub Rings.
`show sub-ring global`	To display global Sub Ring settings.
`copy config running-config nvm profile Test`	To save the updated settings in the configuration profile named **Test** in the non-volatile memory (**nvm**).

Cascaded Sub Rings Example

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

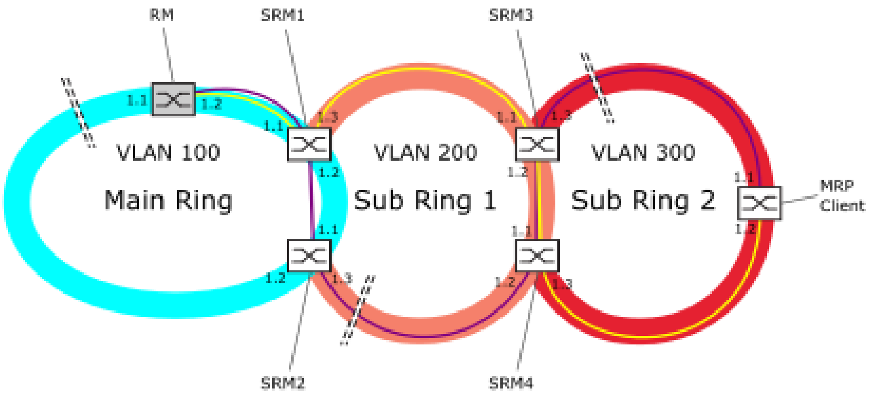
- Set up each device of the Sub Ring configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The following example displays a cascaded Sub Ring network topology which uses the MRP and the SRM protocol. You couple the new network segments as Sub Rings to the existing devices of the main ring.

The following figure presents an example of a cascaded Sub Ring structure:

Example of a



Blue circle: Main ring members in VLAN 100
Orange circle: Sub Ring members in VLAN 200
Red circle: Sub Ring members in VLAN 300
Yellow line: Main network link
Purple line: Redundant network link
Dashed black lines: Blocked network link
SRM1: Sub Ring Manager for Sub Ring 1 and MRP client for the Main Ring
SRM2: Redundant Sub Ring Manager for Sub Ring 1 and MRP client for the Main Ring
SRM3: Redundant Sub Ring Manager for Sub Ring 2 and MRP client for Sub Ring 1
Manager
SRM4: Sub Ring Manager for Sub Ring 2 and MRP client for Sub Ring 1
MRP Client: MRP Client participating in Sub Ring 2
RM: Ring Manager

The configuration for this example is split into the following parts:

- Setting up the Ring Manager mode, page 227
- Setting up the devices participating in the Sub Ring, page 229

Setting Up the *Ring Manager* Mode

This example guides you through the configuration of the *Ring Manager* mode as previously shown. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching > L2-Redundancy > MRP**.
2	Select port ***1/1*** in the Ring port 1 frame and port ***1/2*** in the Ring port 2 frame.
3	Enable the Ring manager function. Select the **On** radio button in the Configuration frame.
4	Assign the value **100** in the **VLAN ID** field.
5	Enable the MRP function. Select the **On** radio button in the Operation frame.
6	To apply the settings, click the ✓ button.
7	Navigate to the **Switching > L2-Redundancy > Spanning Tree > Port**, **CIST** tab.
8	To disable the Spanning Tree function on the ring ports, in the STP active column, clear the checkbox.
9	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain delete`	To delete the MRP domain.
`mrp domain add default-domain`	To add a default MRP domain. Any subsequent MRP domain changes apply to this domain ID.
`mrp domain modify port primary 1/1`	To set up the primary ring port.
`mrp domain modify port secondary 1/2`	To set up the secondary ring port.
`mrp domain modify mode manager`	To enable the Ring manager function.
`mrp domain modify operation enable`	To enable the MRP function.
`mrp domain modify vlan 100`	To assign the VLAN ID to the ring ports.
`interface 1/1 spanning-tree mode disable`	To disable Spanning Tree on interface ***1/1***.
`interface 1/2 spanning-tree mode disable`	To disable Spanning Tree on interface ***1/2***.

Specify a different VLAN membership for the main ring and the Sub Rings. For example, use VLAN ID **100** for the main ring, VLAN ID **200** for the first Sub Ring and VLAN ID **300** for the second Sub Ring.

Setting Up the Devices Participating in the Sub Ring

Set up each device participating in the Sub Ring in the same way. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching > L2-Redundancy > MRP**.
2	From the Port drop-down list, select port ***1/1*** in the Ring port 1 frame and port ***1/2*** in the Ring port 2 frame.
3	Disable the Ring manager function. Select the **Off** radio button in the Operation frame (if this has not already been done).
4	Assign the value **100** in the **VLAN ID** field.
5	Enable the MRP function. Select the **On** radio button in the Operation frame.
6	To apply the settings, click the ✓ button.
7	Navigate to **Switching > L2-Redundancy > FuseNet > Sub Ring**.
8	To add a table row, click the ⊞ button.
9	In the **Name** column, assign a name to the Sub Ring.
10	In the Port column, select the appropriate port for which the device operates in the *Sub Ring Manager* mode. In the given example you use port ***1/3***.
11	Assign the value **200** in the VLAN column.
12	In the Administrative mode column, select the value **manager**. You thus specify which port for coupling the Sub Ring to the main ring becomes the redundant manager. The options for the coupling are: • **manager** When you specify both *Sub Ring Manager* devices with the same value, the device with the greater MAC address manages the redundant link. • **redundant manager** This device manages the redundant link, as long as the other *Sub Ring Manager* device operates in the **manager** mode. Otherwise the device with the greater MAC address manages the redundant link.
13	To activate the Sub Ring, select the checkbox in the Active column.
14	To apply the settings, click the ✓ button.
15	Navigate to the **Switching > L2-Redundancy > Spanning Tree > Port**, **CIST** tab.
16	To disable the Spanning Tree function on the Sub Ring ports, in the STP active column, clear the checkbox.
17	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sub-ring modify 1 port 1/3`	To specify port ***1/3*** as the Sub Ring port.
`sub-ring modify 1 name Test`	To assign the name **Test** to the Sub Ring.
`sub-ring add 1 mode manager vlan 200 port 1/3 name SRM1`	To assign the **manager** mode to the Sub Ring **1**.
`sub-ring enable 1`	To activate the Sub Ring.
`sub-ring operation enable`	To enable the Sub Ring function.
`interface 1/3 spanning-tree mode disable`	To disable Spanning Tree on interface ***1/3***.
`show sub-ring ring`	To display the Sub Ring state on this device.
`show sub-ring global`	To display the Sub Ring global state on this device.

Sub Ring with LAG

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Sub Ring configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

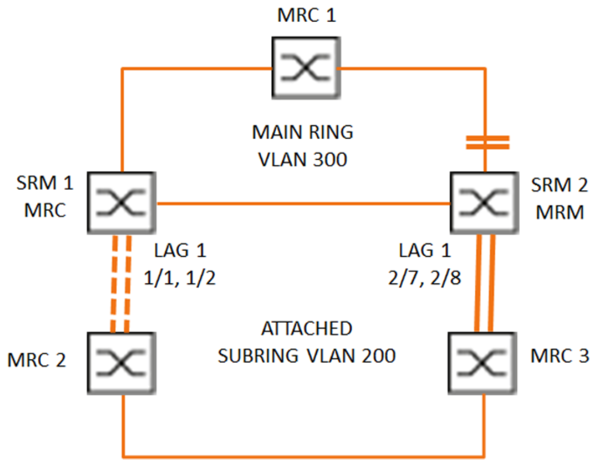
Failure to follow these instructions can result in death, serious injury, or equipment damage.

When at least two parallel redundant connecting lines exist (a trunk) between two devices, and these lines are combined into one logical connection, this is a Link Aggregation (LAG) connection.

The device allows the use of LAG ports as ring ports with the Sub Ring function.

Application Example for Sub Ring with LAG

The following example of Sub Ring with Link Aggregation is a setup between an MRP Ring and a Sub Ring:



The following table describes the device roles as seen in the preceding figure and provides information of how you use the ring ports and Sub Ring ports as LAG ports:

Device name	Ring port	Main Ring role	Sub Ring role	Sub Ring port
MRC1	1/3, 1/4	MRP client	–	–
SRM1	1/3, 1/4	MRP client	Redundant Manager	Lag/1
SRM2	2/4, 2/5	MRP manager	Manager	Lag/1
MRC2	lag/1, 1/3	–	MRP client	–
MRC3	lag/1, 1/3	–	MRP client	–

MRP Ring Configuration

The devices participating in the Main ring are members of VLAN 300.

Execute the following commands for **SRM2**:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain add default-domain`	To add an MRP domain with the ID **default-domain**.
`mrp domain modify port primary 2/4`	To specify port ***2/4*** as ring port **1**.
`mrp domain modify port secondary 2/5`	To specify port ***2/5*** as ring port **2**.
`mrp domain modify mode manager`	To designate the device as the *Ring Manager* device. Do not activate the Ring manager function on any other device.
`mrp domain modify operation enable`	To activate the MRP Ring.
`mrp domain modify vlan 300`	To specify the VLAN ID as **300**.
`mrp operation`	To enable the MRP function in the device.

Execute the following commands for **MRC1, SRM1**:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain add default-domain`	To add an MRP domain with the ID **default-domain**.
`mrp domain modify port primary 1/3`	To specify port ***1/3*** as ring port **1**.
`mrp domain modify port secondary 1/4`	To specify port ***1/4*** as ring port **2**.
`mrp domain modify mode client`	To set up the device as a *Ring Client* device.
`mrp domain modify operation enable`	To activate the MRP Ring.
`mrp domain modify vlan 300`	To specify the VLAN ID as **300**.
`mrp operation`	To enable the MRP function in the device.

Sub Ring Configuration

The devices participating in the attached Sub Ring are members of VLAN 200.

Execute the following commands for **SRM1**:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`link-aggregation add lag/1`	To add a Link Aggregation Group **lag/1**.
`link-aggregation modify lag/1 addport 1/1`	To add port ***1/1*** to the Link Aggregation Group.
`link-aggregation modify lag/1 addport 1/2`	To add port ***1/2*** to the Link Aggregation Group.
`link-aggregation modify lag/1 adminmode`	To activate the Link Aggregation Group.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sub-ring add 1`	To add a Sub Ring with the Sub Ring ID **1**.
`sub-ring modify 1 name SRM1`	To assign the name **SRM1** to the Sub Ring **1**.
`sub-ring modify 1 mode redundant-manager vlan 200 port lag/1`	To assign the device the role of **Sub Ring redundant manager** in Sub Ring **1**. If the Sub Ring is closed, the device blocks the ring port. VLAN **200** is the set for the VLAN ID of the domain. The **lag/1** port is set as a member in VLAN **200**.
`sub-ring enable 1`	To activate Sub Ring **1**.
`sub-ring operation`	To enable the global *Sub Ring Manager* function on this device.

Execute the following commands for **SRM2**:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`link-aggregation add lag/1`	To add a Link Aggregation Group **lag/1**.
`link-aggregation modify lag/1 addport 2/7`	To add port ***2/7*** to the Link Aggregation Group.
`link-aggregation modify lag/1 addport 2/8`	To add port ***2/8*** to the Link Aggregation Group.
`link-aggregation modify lag/1 adminmode`	To activate the Link Aggregation Group.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sub-ring add 1`	To add a Sub Ring with the Sub Ring ID **1**.
`sub-ring modify 1 mode manager vlan 200 port lag/1`	To assign the device the role of **Sub Ring manager** in Sub Ring **1**. VLAN **200** is the set for the VLAN ID of the domain. The **lag/1** port is set as a member in VLAN **200**.
`sub-ring modify 1 name SRM2`	To assign the name **SRM2** to the Sub Ring **1**.
`sub-ring enable 1`	To activate Sub Ring **1**.
`sub-ring operation`	To enable the global *Sub Ring Manager* function on this device.

Execute the following commands for **MRC 2, 3**:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain add default-domain`	To add an MRP domain with the ID **default-domain**.
`mrp domain modify port primary lag/1`	To specify port **lag/1** as ring port **1**.
`mrp domain modify port secondary 1/3`	To specify port ***1/3*** as ring port **2**.
`mrp domain modify mode client`	To set up the device as a *Ring Client* device.
`mrp domain modify operation enable`	To activate the MRP Ring.
`mrp domain modify vlan 200`	To specify the VLAN ID as **200**.
`mrp operation`	To enable the MRP function in the device.

Disabling STP

Disable the Spanning Tree function on every port that you specified as an MRP or Sub Ring port. The following example uses port ***1/3***.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/3`	To change to the Interface Configuration mode of interface ***1/3***.
`no spanning-tree operation`	To disable the Spanning Tree function on the port.

Ring/Network Coupling Function

Based on a ring, the Ring/Network Coupling function couples rings or network segments redundantly. Ring/Network Coupling connects 2 rings/network segments through 2 separate paths.

When the devices in the coupled network are Schneider Electric devices, the Ring/Network Coupling function supports the coupling following ring protocols in the primary and secondary rings:

- HIPER Ring
- Fast HIPER Ring
- MRP

The Ring/Network Coupling function can also couple network segments of a bus and mesh structures.

Methods of Ring/Network Coupling

1-Switch Coupling

Two ports of **one** device in the first ring/network connect to one port each of two devices in the second ring/network. Example of 1-Switch coupling1: Ring2: Backbone3: Partner coupling port4: Coupling port5: Main line6: Redundant line

In the 1-Switch coupling method, the main line forwards data and the device blocks the redundant line.

When the main line no longer functions, the device immediately unblocks the redundant line. When the main line is restored, the device blocks data on the redundant line. The main line forwards data again.

The ring coupling detects and handles an error within 500 ms (typically 150 ms).

2-Switch Coupling

One port each from **two** devices in the first ring/network connects to one port each of two devices in the second ring/network segment. Example of 2-Switch coupling1: Ring2: Backbone3: Main line4: Redundant line

The device with the redundant line connected and the device with the main line connected use control packets to inform each other about their operating states, using the existing network or a dedicated control line.

When the main line goes down, the redundant device (Stand-by) unblocks the redundant line. When the main line comes up again, the device connected to the main line informs the redundant device of this. The Stand-by device then blocks data on the redundant line. The device connected to the main line then forwards data on the main line.

The ring coupling detects and handles an error within 500 ms (typically 150 ms).

Selection of a Coupling Method

The type of coupling configuration is primarily determined by the network topological and the desired level of availability.

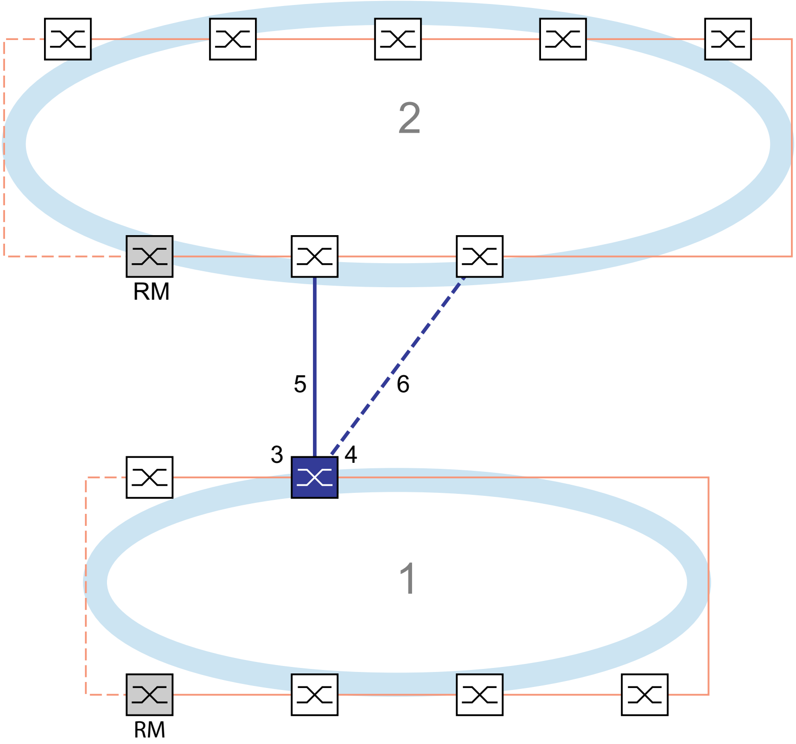
The following table presents the selection criteria for the configuration types for redundant coupling

Selection criteria	**1-Switch coupling**	**2-Switch coupling**	**2-Switch coupling with Control line**
Application	The 2 devices are in impractical topological positions. Therefore, putting a link between the devices would involve a lot of effort for 2-Switch coupling.	The 2 devices are in practical topological positions. Installing a control line would involve a lot of effort.	The 2 devices are in practical topological positions. Installing a control line would not involve much effort.
Disadvant-age	If the Switch set up for the redundant coupling becomes inoperable, no connection remains between the networks.	More effort is needed to connect both devices to the network (compared with 1-Switch coupling).	More effort is needed to connect both devices to the network (compared with 1-Switch and 2-Switch coupling).
Advantage	Less effort involved in connecting the 2 devices to the network (compared with 2-Switch coupling).	When one of the devices set up for the redundant coupling becomes inoperable, the coupled networks are still connected.	When one of the devices set up for the redundant coupling becomes inoperable, the coupled networks are still connected. The partner determination between the coupling devices occurs more reliable and faster than without the control line.

Advanced Information

Link Topology of 1-Switch Coupling

The following figure presents an example of 1-Switch coupling:



1: Ring
2: Backbone
3: Partner coupling port
4: Coupling port
5: Main line
6: Redundant line

In a 1-Switch coupling Example of 1-Switch coupling1: Ring2: Backbone3: Partner coupling port4: Coupling port5: Main line6: Redundant line, one device manages both coupling lines:

- The partner coupling port (3) connects the main line (5).
- The coupling port (4) connects the redundant line (6).

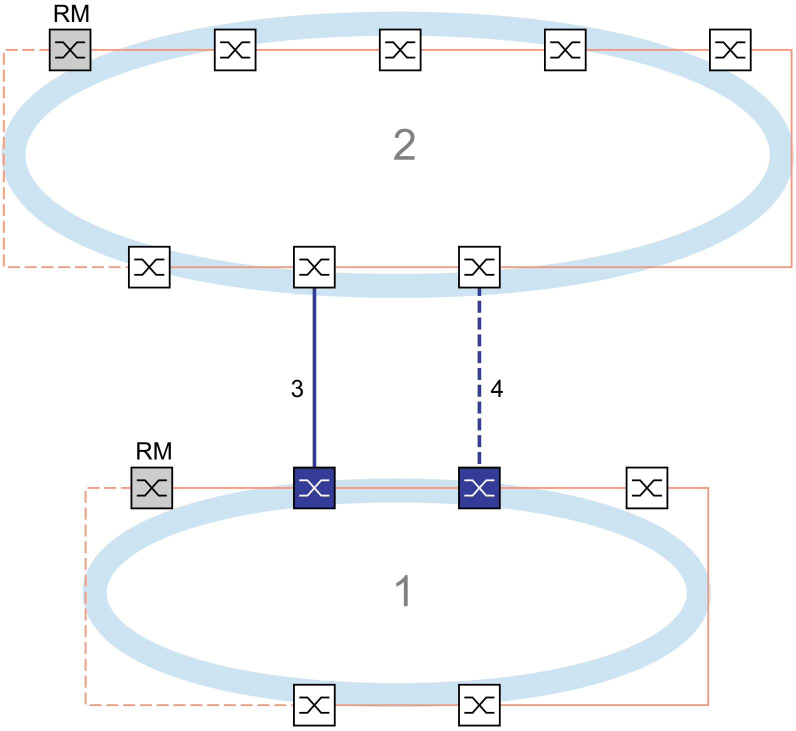
The single coupling device sends the following test packets:

- The partner coupling port (3) sends Ring/Network Coupling unicast test packets A.
- The coupling port (4) sends Ring/Network Coupling unicast test packets B.

  NOTE: The 2 ring ports (unnumbered) connect the local redundant ring (red lines in graphic) and do not send any Ring/Network Coupling test packets.

Link Topology of 2-Switch Coupling

The following figure presents an example of 2-Switch coupling:



1: Ring
2: Backbone
3: Main line
4: Redundant line

In a 2-Switch coupling Example of 2-Switch coupling1: Ring2: Backbone3: Main line4: Redundant line, the 2 devices have specific roles:

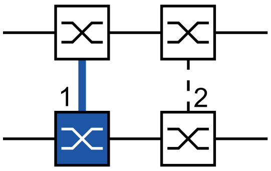
- The coupling port (1) of the primary device connects the main line 2-Switch coupling, Primary device1: Coupling port2: Partner coupling port.
- The partner coupling port (1) of the secondary device connects the stand-by line (4) 2-Switch coupling, Stand-by device1: Coupling port2: Partner coupling port.

The primary device 2-Switch coupling, Primary device1: Coupling port2: Partner coupling port sends no test packets.

The secondary device 2-Switch coupling, Stand-by device1: Coupling port2: Partner coupling port sends the following test packets:

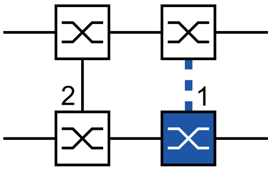
- The 2 ring ports (unnumbered) send Ring/Network Coupling unicast test packets A.
- The coupling port (4) sends Ring/Network Coupling unicast test packets B.

The following figure presents an example of 2-Switch coupling with a primary device:



1: Coupling port
2: Partner coupling port

The following figure presents an example of 2-Switch coupling with a stand-by device:

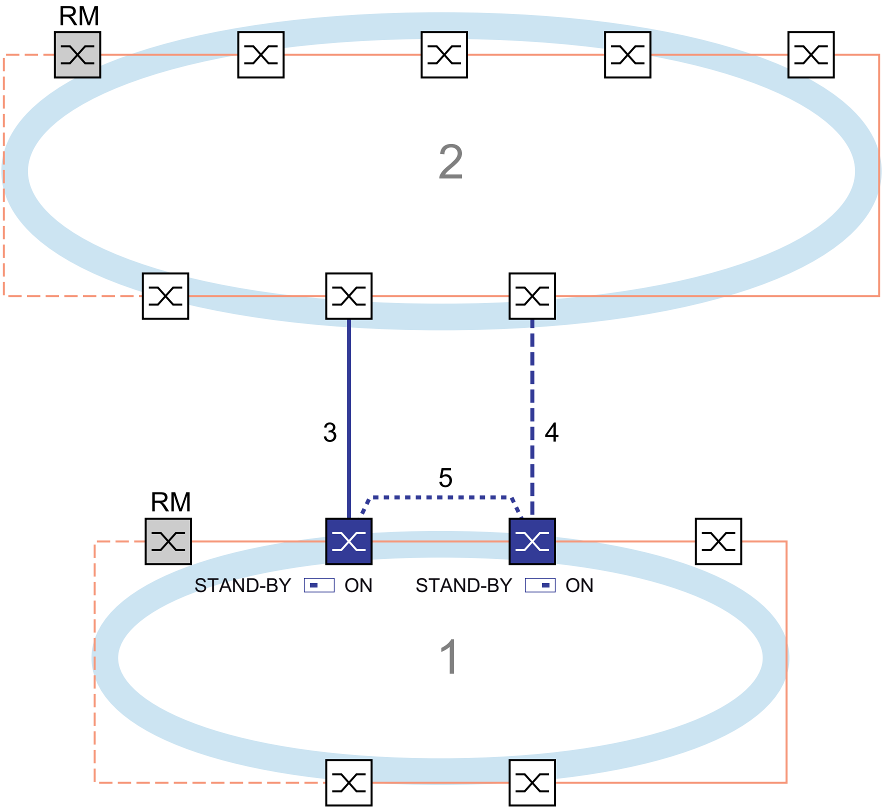


1: Coupling port
2: Partner coupling port

Link Topology of 2-Switch Coupling with Control Line

This topology differs from the previous one by the additional control line. The control line helps accelerate reconfiguration.

The following figure presents an example of 2-Switch coupling with control line:



1: Ring
2: Backbone
3: Main line
4: Redundant line
5: Control line

In a 2-Switch coupling with Control Line Example of 2-Switch coupling with control line1: Ring2: Backbone3: Main line4: Redundant line5: Control line, both devices are connected as follows:

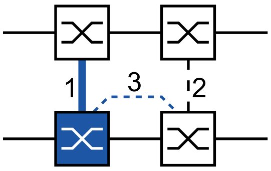
- The primary device and the secondary device connect the control line (5) through their control ports (unnumbered).
- The coupling port (1) of the primary device connects the main line 2-Switch coupling with Control Line, Primary device1: Coupling port2: Partner coupling port3: Control line.
- The partner coupling port (1) of the secondary device connects the stand-by line (4) 2-Switch coupling with Control Line, Stand-by device1: Coupling port2: Partner coupling port3: Control line.

The primary device 2-Switch coupling with Control Line, Primary device1: Coupling port2: Partner coupling port3: Control line sends control packets on its control port.

The secondary device 2-Switch coupling with Control Line, Stand-by device1: Coupling port2: Partner coupling port3: Control line sends the following packets:

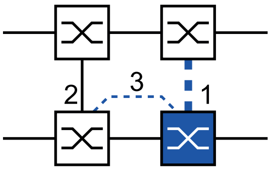
- The control port (unnumbered) sends control packets.
- The 2 ring ports (unnumbered) send Ring/Network Coupling unicast test packets A.
- The coupling port (4) sends Ring/Network Coupling unicast test packets B.

The following figure presents an example of 2-Switch coupling with a control line and a primary device:



1: Coupling port
2: Partner coupling port
2: Control line

The following figure presents an example of 2-Switch coupling with a control line and a stand-by device:



1: Coupling port
2: Partner coupling port
2: Control line

Packets

The Ring/Network Coupling function uses *Test*, *Control*, *Link Change*, and *Topology Change* packets.

The following table describes the *Ring/Network Coupling* packets:

Packet Type	Send Mode	Time Parameter	Value
Unicast test packet A [1]	Cyclical	Send interval	80 ms (50 ms during config. phase)
		Reception timeout	1500 ms
Unicast test packet B [2]	Cyclical	Send interval	80 ms (50 ms during config. phase)
		Reception timeout	1500 ms
Control packet[3]	Event-driven	On reconfiguration	–
Link Change packet[4]	Event-driven	On link-down or link-up of a ring port or coupling port	–
Topology Change packet	Event-driven	On reconfiguration	–

[1] 2-Switch coupling: Sent by the secondary (stand-by) device only. Destination address: Device MAC address+1, source address: Device MAC address+2.

[2] 2-Switch coupling: Sent by the secondary (stand-by) device only. Destination address: Device MAC address+2, source address: Device MAC address+1 (addresses swapped with respect to unicast test packet A).

[3] Destination address (multicast): 01:80:63:07:00:02, source address: 00:80:63:07:10:01.

[4] Sent by supporting ring participants.

1-Switch coupling: The local device periodically sends test packets A into the ring from both ring ports. The local device expects to receive the test packets A back on its respective other ring port. If the local device receives no test packets A for a specified amount of time, the local device detects a network interruption.

The local device also sends test packets B from its partner coupling port. The test packets B are special packets that the local device receives at the coupling port although the coupling port blocks the reception of normal packets. The local device expects to receive the test packets B back on its coupling port. If the local device receives no test packets B for a specified amount of time, the local device detects a coupling network interruption.

2-Switch coupling: The secondary (stand-by) device periodically sends test packets A into the ring from both ring ports. The secondary device expects to receive the test packets A back on its respective other ring port. If the secondary device receives no test packets A for a specified amount of time, the secondary device detects a network interruption.

The secondary (stand-by) device also sends test packets B from its coupling port. The test packets B are special packets that the secondary device sends from its coupling port although the coupling port blocks the sending of normal packets. The primary device forwards received test packets B to the secondary device. The secondary device expects to receive the test packets B back on its ring port connected to the primary device. If the secondary device receives no test packets B for a specified amount of time, the secondary device detects a coupling network interruption.

In extended redundancy mode, the same packets are used, only the reaction to a detected network interruption differs.

On reconfiguration of the Ring/Network coupling, the secondary (stand-by) device flushes its MAC address table (forwarding database) and sends Ring/Network coupling *Topology Change* packets to its partner device. It also sends Ring/Network coupling *Topology Change* packets to the connected rings.

If a device participating in a connected ring receives a Ring/Network coupling *Topology Change* packet, it flushes its MAC address table (forwarding database).

It also converts the Ring/Network coupling *Topology Change* packet to a ring *Topology Change* packet and sends the *Topology Change* packet on. The *Topology Change* packets also prompt the other devices participating in the ring to flush their MAC address table (forwarding database). This applies to all rings that the Ring/Network coupling connects. This procedure helps forward the payload packets over the new path.

The Ring/Network coupling devices also act on ring *Topology Change* packets from a *Ring Manager* device because the Ring/Network coupling devices are members of that ring.

Packet Prioritization

The Ring/Network Coupling devices send their test packets, control packets, *Link Down* packets, and Ring/Network coupling *Topology Change* packets with the fixed VLAN ID 1. In the default setting, these packets are untagged and thus without priority (Class of Service) information. To help minimize the reconfiguration time under high network load, you can add a VLAN tag and thus priority information to these packets. The devices then send and forward the packets with the IEEE 802.1Q Class of Service priority 7 (Network control).

To prioritize these packets, set up each of the following ports as **T** (tagged) member of VLAN 1:

- In the local ring where the coupling device (or devices) are located:
  - The coupling port of the respective coupling device (local or secondary)
  - The partner coupling port of the respective coupling device (local or primary)
  - The ring ports of all devices in the local ring, including the *Ring Manager* device
- In the remote ring:
  - The port of the device in the remote ring connected to the coupling port
  - The port of the device in the remote ring connected to the partner coupling port
  - The 2 ring ports connecting the 2 devices just mentioned to each other

  NOTE: Confirm that the VLAN membership settings of both control ports match in a 2-Switch coupling with Control Line. You can keep the default settings of the control ports (VLAN 1 membership untagged).

Link Topology Requirements

In the absence of packet prioritization, confirm that the following links are direct, without any intervening devices:

- The 2 coupling links connecting the coupling device (or devices) in the local ring with the 2 coupled devices in the remote ring
- The link in the remote ring connecting the 2 coupled devices
- In a 2-Switch coupling: The link in the local ring connecting the 2 coupling devices
- In a 2-Switch coupling with Control Line, use a direct line.

This helps ensure that the packets are transmitted with minimal delay and high reliability. This again helps minimize the reconfiguration time under high network load.

NOTE: Use the link topology, previously described, even with packet prioritization.

Prepare the Ring/Network Coupling

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the Ring/Network Coupling configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.
- Use the Ring/Network Coupling function only on ports on which the Rapid Spanning Tree Protocol (RSTP) is inactive.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Using the images in the dialog, you define the role of the devices within the Ring/Network Coupling.

These conventions are used in the screenshots and diagrams in this section:

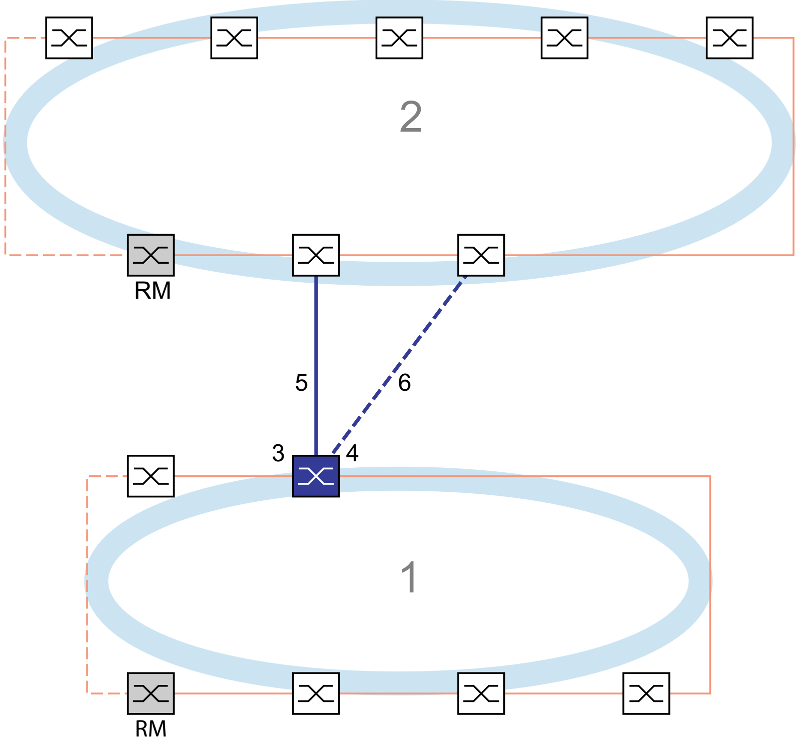
- Blue boxes and lines indicate devices or connections of the items being described.
- Solid lines indicate a main connection.
- Dash lines indicate a stand-by connection.
- Dotted lines indicate the control line.

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **L2-Redundancy** > **FuseNet** > **Ring/Network Coupling**.
2	In the Mode frame, Type option list, select the required radio button. • **one-switch coupling** • **two-switch coupling, master** • **two-switch coupling, slave** • **two-switch coupling with control line, master** • **two-switch coupling with control line, slave**

1-Switch Coupling

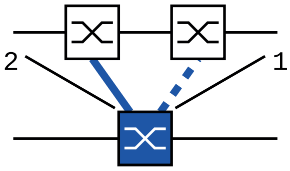
The following figure presents an example of 1-Switch coupling:



1: Ring
2: Backbone
3: Partner coupling port
4: Coupling port
5: Main line
6: Redundant line

The main line, indicated by the solid blue line, which is connected to the partner coupling port provides coupling between the two networks in the normal mode of operation. If the main line is inoperable, the redundant line, indicated by the dashed blue line, which is connected to the coupling port takes over the ring/ network coupling. One switch performs the coupling switch-over.

The following settings of 1-switch coupling apply to the device displayed in blue in the selected graphic:



1: Coupling port
2: Partner coupling port

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **L2-Redundancy** > **FuseNet** > **Ring/Network Coupling**.
2	In the Mode frame, Type option list, select the **one-switch coupling** radio button. **NOTE:** Set up the Partner coupling port and the ring ports on different ports.
3	In the Coupling port frame, select the port on which you want to connect the redundant line from the Port drop-down list.
4	In the Partner coupling port frame, select the port on which you connect the main line from the Port drop-down list.
5	Enable the Ring/Network Coupling function. Select the **On** radio button in the Operation frame.
6	To apply the settings, click the ✓ button.
7	Connect the redundant line to the Partner coupling port. In the Partner coupling port frame, the **State** field displays the status of the Partner coupling port.
8	Connect the main line to the Coupling port. In the Coupling port frame, the **State** field displays the status of the Coupling port.
9	In the Information frame, the **Redundancy** field displays if the redundancy is available. The **Configuration failure** field displays if the settings are complete and correct.

For the coupling ports, perform the following steps:

Step	Action
1	Navigate to the **Basic Settings** > **Port**, **Configuration** tab.
2	For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
3	To apply the settings, click the ✓ button.

To minimize the ring recovery time in case of a link-up after an interruption, set up the speed and duplex mode of the ring ports as follows:

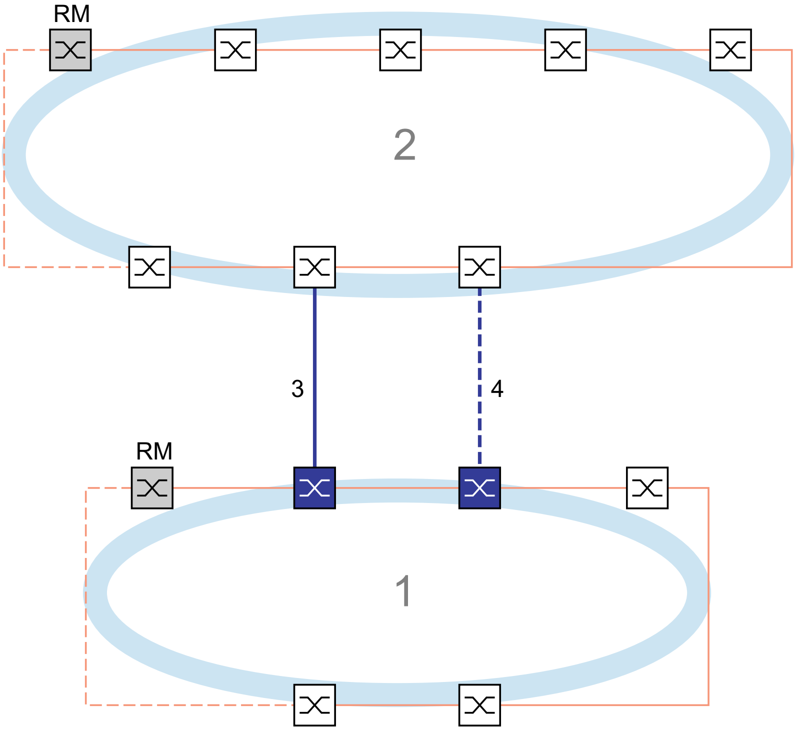
- For 100 Mbit/s TX ports, disable Automatic Negotiation and manually specify 100M FDX.
- For the other port types, keep the port-specific default settings.

If you have set up VLANs on the coupling ports, you must specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching > VLAN > Port**.
2	Change the Port-VLAN ID setting to the value of the VLAN ID set up on the ports.
3	Clear the Ingress filtering checkbox for both coupling ports.
4	Navigate to **Switching > VLAN > Configuration**.
5	To tag the redundant connections for **VLAN 1** and VLAN Membership, enter the value **T** in the cells corresponding to both coupling ports on the **VLAN 1** table row.
6	To apply the settings, click the ✓ button. The coupling device now sends the redundancy packets with the highest priority on **VLAN 1**.
7	In the Configuration frame Redundancy mode option list, specify the type of redundancy: • With the redundant ring/network coupling setting, either the main line or the redundant line is active. The setting allows the addition of toggle between both lines. • When you activate the extended redundancy setting, the main line and the redundant line can become active simultaneously if required. The setting allows the addition of redundancy to the remote (coupled) network. When the connection between the coupling devices in the second network becomes inoperable, the coupling devices continue to transmit and receive data. **NOTE:** During the reconfiguration period, packet duplications can occur. Therefore, select this setting only if your devices detect package duplications.
8	The Coupling mode describes the type of the backbone network to which you connect the ring network (example of 1-Switch coupling): In the Configuration frame, Coupling mode option list, specify the type of the second network: • If you connect to a ring network, select the **ring coupling** radio button. • If you connect to a bus or mesh structure, select the network coupling radio button.
9	To apply the settings, click the ✓ button.
10	To reset the coupling settings to the default state, click the 🗑 button.

2-Switch Coupling

The following figure presents an example of 2-Switch coupling:



1: Ring
2: Backbone
3: Main line
4: Redundant line

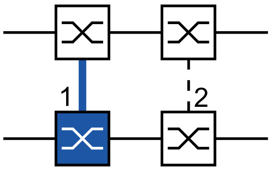
The coupling between 2 networks is performed by the main line, indicated by the solid blue line. If the main line or one of the connected devices becomes inoperable, the redundant line, indicated by the dashed black line, takes over the network coupling. The coupling is performed by 2 devices.

The devices send control packets to each other over the network.

The primary device connected to the main line, and the stand-by device connected to the redundant line are partners with regard to the coupling. Connect the 2 partners using the ring ports.

2-Switch Coupling, Primary Device

The following settings of 2-Switch coupling apply to the device displayed in blue in the selected graphic:



1: Coupling port
2: Partner coupling port

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **L2-Redundancy** > **FuseNet** > **Ring/Network Coupling**.
2	In the Mode frame, Type option list, select the **two-switch coupling, master** radio button.
3	In the Coupling port frame, select the port on which you connect the network segments from the Port drop-down list. Set up the Coupling port and the ring ports on different ports.
4	Enable the Ring/Network Coupling function. Select the **On** radio button in the Operation frame.
5	To apply the settings, click the ✓ button.
6	Connect the main line to the Coupling port. In the Coupling port frame, the **State** field displays the status of the Coupling port. When the partner is already operating in the network, the **IP address** field in the Partner coupling port frame displays the IP address of the partner port.
7	In the Information frame, the **Redundancy** field displays if the redundancy is available. The **Configuration failure** field displays if the settings are complete and correct.
8	To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to **off**: • disable the operation • change the configuration

For the coupling ports, perform the following steps:

Step	Action
1	Navigate to the **Basic Settings** > **Port**, **Configuration** tab.
2	For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
3	To apply the settings, click the ✓ button.

To minimize the ring recovery time in case of a link-up after an interruption, set up the speed and duplex mode of the ring ports as follows:

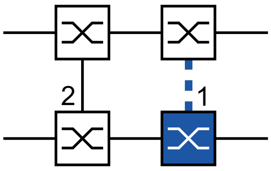
- For 100 Mbit/s TX ports, disable Automatic Negotiation and manually specify 100M FDX.
- For the other port types, keep the port-specific default settings.

If you have set up VLANs on the coupling ports, you must specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching** > **VLAN** > **Port**.
2	Change the Port-VLAN ID setting to the value of the VLAN ID set up on the ports.
3	Clear the Ingress filtering checkbox for both coupling ports.
4	Navigate to **Switching** > **VLAN** > **Configuration**.
5	To tag the redundant connections for **VLAN 1** and to establish the VLAN membership, enter the value **T** in the cells corresponding to both coupling ports on the **VLAN 1** table row.
6	To apply the settings, click the ✓ button. The coupling device now sends the redundancy packets with the highest priority on **VLAN 1**.

2-Switch Coupling, Stand-by Device

The following settings of 2-Switch coupling, stand-by device, apply to the device displayed in blue in the selected graphic:



1: Coupling port
2: Partner coupling port

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **L2-Redundancy** > **FuseNet** > **Ring/Network Coupling**.
2	In the Mode frame, Type option list, select the **two-switch coupling, slave** radio button.
3	In the Coupling port frame, select the port on which you connect the network segments from the Port drop-down list. Set up the Coupling port and the ring ports on different ports.
4	Enable the Ring/Network Coupling function. Select the **On** radio button in the Operation frame.
5	To apply the settings, click the ✓ button.
6	Connect the redundant line to the Coupling port. In the Coupling port frame, the **State** field displays the status of the Coupling port. When the partner is already operating in the network, the **IP address** field in the Partner coupling port frame displays the IP address of the partner port. In the Information frame, the **Redundancy** field displays if the redundancy is available. The **Configuration failure** field displays if the settings are complete and correct.
7	To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to **off**: • disable the operation • change the configuration

For the coupling ports, perform the following steps:

Step	Action
1	Navigate to the **Basic Settings** > **Port**, **Configuration** tab.
2	For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
3	To apply the settings, click the ✓ button.

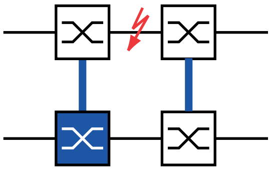
To minimize the ring recovery time in case of a link-up after an interruption, set up the speed and duplex mode of the ring ports as follows:

- For 100 Mbit/s TX ports, disable Automatic Negotiation and manually specify 100M FDX.
- For the other port types, keep the port-specific default settings.

If you have set up VLANs on the coupling ports, you must specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

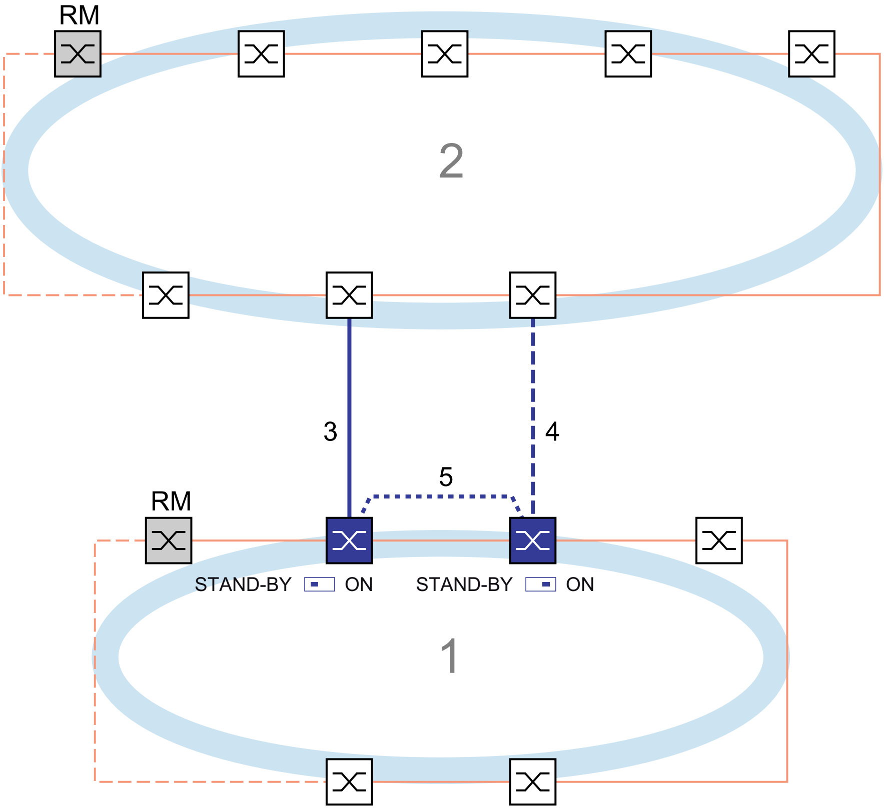
Step	Action
1	Navigate to **Switching** > **VLAN** > **Port**.
2	Change the Port-VLAN ID setting to the value of the VLAN ID set up on the ports.
3	Clear the Ingress filtering checkbox for both coupling ports.
4	Navigate to **Switching** > **VLAN** > **Configuration**.
5	To tag the redundant connections for **VLAN 1** and VLAN Membership, enter the value **T** in the cells corresponding to both coupling ports on the **VLAN 1** table row.
6	To apply the settings, click the ✓ button. The coupling devices now send the redundancy packets with the highest priority on **VLAN 1**.

Specify the Redundancy mode and Coupling mode settings. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching** > **L2-Redundancy** > **FuseNet** > **Ring/Network Coupling**.
2	In the Configuration frame, Redundancy mode option list, select one of the following radio buttons: • **redundant ring/network coupling** With this setting, either the main line or the redundant line is active. The setting allows devices to toggle between both lines. • **extended redundancy** With this setting, the main line and the redundant line are active simultaneously. The setting allows the addition of redundancy to the second network. When the connection between the coupling devices in the second network becomes inoperable, the coupling devices continue to transmit and receive data.  During the reconfiguration period, packet duplications can occur. Therefore, select this setting only if your devices detect package duplications.
3	In the Configuration frame, Coupling mode option list, select one of the following radio buttons: • If you connect to a ring network, select the **ring coupling** radio button. • If you connect to a bus or mesh structure, select the network coupling radio button. The Coupling mode describes the type of the backbone network to which you connect the ring network. Example of 2-Switch coupling1: Ring2: Backbone3: Main line4: Redundant line
4	To apply the settings, click the ✓ button.
5	To reset the coupling settings to the default state, click the 🗑 button.

2-Switch Coupling with Control Line

The following figure presents an example of 2-Switch coupling with a control line:



1: Ring
2: Backbone
3: Main line
4: Redundant line
5: Control Line

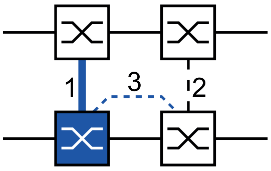
The coupling between 2 networks is performed by the main line, indicated by the solid blue line. If the main line or one of the adjacent devices become inoperable, the redundant line, indicated by the dashed blue line, takes over coupling the 2 networks. The ring coupling is performed by 2 devices.

The devices send control packets over a control line indicated by the dotted blue line. 2-Switch coupling with Control Line, Primary device1: Coupling port2: Partner coupling port3: Control line

The primary device connected to the main line, and the stand-by device connected to the redundant line are partners with regard to the coupling. Connect the 2 partners using the ring ports.

2-Switch Coupling with Control Line, Primary Device

The following settings of 2-Switch coupling with a control line for a primary device apply to the device displayed in blue in the selected graphic:



1: Coupling port
2: Partner coupling port
2: Control line

Perform the following steps:

Step	Action
1	Navigate to **Switching > L2-Redundancy > FuseNet > Ring/Network Coupling**.
2	In the Mode frame, Type option list, select the **two-switch coupling with control line, master** radio button.
3	In the Coupling port frame, select the port on which you connect the network segments from the Port drop-down list. Set up the Coupling port and the ring ports on different ports.
4	In the Control port frame, select the port on which you connect the control line from the Port drop-down list. Set up the Coupling port and the ring ports on different ports.
5	Enable the Ring/Network Coupling function. Select the **On** radio button in the Operation frame.
6	To apply the settings, click the ✓ button.
7	Connect the redundant line to the Coupling port. In the Coupling port frame, the **State** field displays the status of the Coupling port. When the partner is already operating in the network, the **IP address** field in the Partner coupling port frame displays the IP address of the partner port.
8	Connect the control line to the Control port. In the Control port frame, the **State** field displays the status of the Control port. When the partner is already operating in the network, the **IP address** field in the Partner coupling port frame displays the IP address of the partner port. In the Information frame, the **Redundancy** field displays if the redundancy is available. The **Configuration failure** field displays if the settings are complete and correct.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to **off**:

- Disable the operation
- Change the configuration

For the coupling ports, perform the following steps:

Step	Action
1	Navigate to the **Basic Settings > Port**, **Configuration** tab.
2	For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
3	To apply the settings, click the ✓ button.

To minimize the ring recovery time in case of a link-up after an interruption, set up the speed and duplex mode of the ring ports as follows:

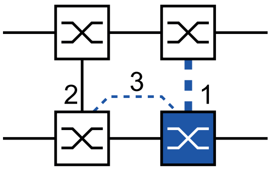
- For 100 Mbit/s TX ports, disable Automatic Negotiation and manually specify 100M FDX.
- For the other port types, keep the port-specific default settings.

If you have set up VLANs on the coupling ports, you must specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching** > **VLAN** > **Port**.
2	Change the Port-VLAN ID setting to the value of the VLAN ID set up on the ports.
3	Clear the Ingress filtering checkbox for both coupling ports.
4	Navigate to **Switching** > **VLAN** > **Configuration**.
5	To tag the redundant connections for **VLAN 1** and VLAN Membership, enter the value **T** in the cells corresponding to both coupling ports on the **VLAN 1** table row.
6	To apply the settings, click the ✓ button. The coupling device now sends the redundancy packets with the highest priority on **VLAN 1**.

2-Switch Coupling with Control Line, Stand-by Device

The following settings of 2-Switch coupling with a control line, a stand-by device, apply to the device displayed in blue in the selected graphic:



1: Coupling port
2: Partner coupling port
2: Control line

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **L2-Redundancy** > **FuseNet** > **Ring/Network Coupling**.
2	In the Mode frame, Type option list, select the **two-switch coupling with control line, slave** radio button.
3	In the Coupling port frame, select the port on which you connect the network segments from the Port drop-down list. Set up the Coupling port and the ring ports on different ports.
4	In the Control port frame, select the port on which you connect the control line from the Port drop-down list. Set up the Coupling port and the ring ports on different ports.
5	Enable the Ring/Network Coupling function. Select the **On** radio button in the Operation frame.
6	To apply the settings, click the ✓ button.
7	Connect the redundant line to the Coupling port. In the Coupling port frame, the **State** field displays the status of the Coupling port. When the partner is already operating in the network, the **IP address** field in the Partner coupling port frame displays the IP address of the partner port.
8	Connect the control line to the Control port. In the Control port frame, the **State** field displays the status of the Control port. When the partner is already operating in the network, the **IP address** field in the Partner coupling port frame displays the IP address of the partner port. In the Information frame, the **Redundancy** field displays if the redundancy is available. The **Configuration failure** field displays if the settings are complete and correct.

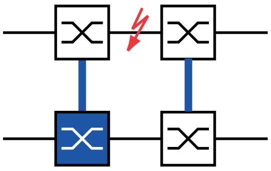
To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to **off**:

- Disable the operation
- Change the configuration

For the coupling ports, perform the following steps:

Step	Action
1	Navigate to **Switching** > **VLAN** > **Port**.
2	Change the Port-VLAN ID setting to the value of the VLAN ID set up on the ports.
3	Clear the Ingress filtering checkbox for both coupling ports.
4	Navigate to **Switching** > **VLAN** > **Configuration**.
5	To tag the redundant connections for **VLAN 1** and VLAN Membership, enter the value **T** in the cells corresponding to both coupling ports on the **VLAN 1** table row.
6	To apply the settings, click the ✓ button. The coupling devices now send the redundancy packets with the highest priority on **VLAN 1**.

Specify the Redundancy mode and Coupling mode settings. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching > L2-Redundancy > FuseNet > Ring/Network Coupling**.
2	In the Configuration frame, Redundancy mode option list, select one of the following radio buttons: • **redundant ring/network coupling** With this setting, either the main line or the redundant line is active. The setting allows devices to toggle between both lines. • **extended redundancy** With this setting, the main line and the redundant line are active simultaneously. The setting allows the addition of redundancy to the second network. When the connection between the coupling devices in the second network becomes inoperable, the coupling devices continue to transmit and receive data.  During the reconfiguration period, packet duplications can occur. Therefore, select this setting only if your devices detect package duplications.
3	In the Configuration frame, Coupling mode option list, select one of the following radio buttons: • If you connect to a ring network, select the **ring coupling** radio button. • If you connect to a bus or mesh structure, select the network coupling radio button. The Coupling mode describes the type of the backbone network to which you connect the ring network (refer to an example of 2-Switch coupling with a control line).
4	To apply the settings, click the ✓ button.
5	To reset the coupling settings to the default state, click the 🗑 button.

RCP Function

Industrial applications require the networks to have high availability. This includes deterministic, short interruption times in cases where a network device or link becomes inoperable.

A ring topology provides short transition times with a minimal use of resources. However, ring topologies bring the challenge of coupling these rings redundantly.

The Redundant Coupling Protocol (RCP) allows the coupling of rings that are operating with one of the following redundancy protocols:

- MRP
- HIPER Ring
- RSTP

The RCP function also allows the coupling of multiple secondary rings to a primary ring. See the following figure. Only the devices which couple the rings require the RCP function.

You can also use devices other than Schneider Electric devices within the coupled networks.

The RCP function uses a master and a slave device to transport data between the networks. Only the master device forwards frames between the rings.

Using Schneider Electric proprietary multicast messages, the RCP master and slave devices inform each other about their operating state. Set up the devices in the secondary ring which are not coupling devices to forward the following multicast addresses:

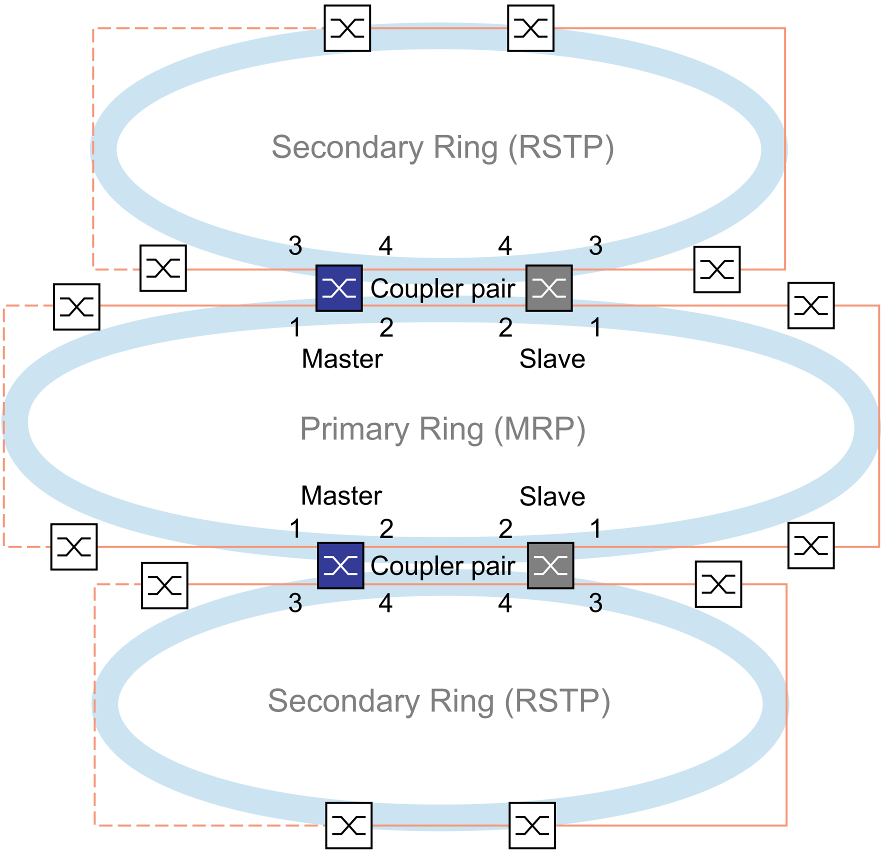
- **01:80:63:07:00:09**
- **01:80:63:07:00:0A**

Connect the master and slave devices as direct neighbors.

You use 4 ports per device to establish the redundant coupling. Set up the coupling devices with 2 inner and 2 outer ports in each network.

- The inner ports connect the master and slave devices.
- The outer ports connect the devices to the other, neighboring devices of the network.

The following figure presents an example of a 2-Switch redundant coupling (2 coupler pairs):



1: Outer coupling port in the primary ring
2: Inner coupling port in the primary ring
3: Outer coupling port in the secondary ring
4: Inner coupling port in the secondary ring

When you specify the role of a coupler device as auto, the coupler device automatically selects its role as master or slave. When you want a predetermined master or slave device, specify the roles explicitly.

If the master is no longer reachable using the inner coupling ports, the slave device waits for a specified timeout period to expire before taking over the master role. During the timeout period, the slave attempts to reach the master using the outer coupling ports. When the master is still unreachable, the slave assumes the master role. To maintain stability in the network connected to the outer coupling ports, specify the timeout period for a longer duration than the recovery time in the coupled rings.

> **NOTE:** Disable RSTP on the RCP inner and outer ports that are not connected to the RSTP ring. In the example configuration, you disable RSTP on ports **1** and **2** of every device.

Prerequisites for RCP

Prerequisite for setting up an RCP coupler pair is that every device in the network (besides the coupler pair) supports the forwarding of untagged multicast packets.

Advanced Information

Topology Overview

RCP supports the 2-Switch Redundant Coupling topology.

NOTE: For a topology example with 2 instances of a 2-Switch Redundant Coupling (refer to an example of a 2-Switch redundant coupling (2 coupler pairs)).

This topology has the following characteristics:

- Each RCP device has 2 internal network segments:
  - A primary segment
  - A secondary segment
- In the normal state of operation, the RCP devices treat packets traveling between these 2 network segments as follows:
  - The RCP master device forwards packets between the 2 network segments.
  - The RCP slave device does **not** forward packets between the 2 network segments.
- Port associations:
  - Only the ports explicitly set up as inner or outer RCP ports for the secondary segment belong to the RCP secondary segment of the device.
  - The inner and outer RCP ports for the primary segment belong to the RCP primary segment.
  - All other ports implicitly belong to the RCP primary segment.
- The management of an RCP device is located in the primary segment.

  NOTE: If you want to access the management of an RCP slave device from the secondary segment, avoid the port-based routing function on the outer ports for the secondary segment. This helps you maintain the management access to the device from the secondary segment.

Topology of the 2-Switch Redundant Coupling

In a 2-Switch Redundant Coupling, one pair of devices couples the 2 rings. Each of the paired devices has a distinct coupling role master or slave, either automatically set up or explicitly specified.

The devices are connected as follows (refer to an example of a 2-Switch redundant coupling (2 coupler pairs)):

- The ring ports (1) of both devices connect to the primary ring/network. These ports are the outer ports for the primary network.
- The ring ports (2) of both devices connect to each other for the primary ring/network. These ports are the inner ports for the primary network.
- The ring ports (3) of both devices connect to the secondary ring/network. These ports are the outer ports for the secondary network.
- The ring ports (4) of both devices connect to each other for the secondary ring. These ports are the inner ports for the secondary network.

Packets

RCP uses multicast test packets, named after the RCP port role number (1..4) of the sending port.

The following table describes RCP packets:

Packet Type	Operating State	Time Parameter	Value
Test packets 2 and 4 (on the inner ports)	Normal operation of the inner ports	Send interval	45 ms
		Reception timeout[1]	180 ms (4 send intervals, fixed)
Test packets 1 and 3 (on the outer ports)	On link interruption of the inner ports	Send interval	10 ms (during the first 90 ms of the reception timeout) 5 ms (after 90 ms of the reception timeout have elapsed)
		Topology Change timeout[2]	5 ms..60000 ms (customizable, default setting: 250 ms)

[1] The slave treats the reception timeout as a link interruption on the respective port even if the port still has a link.

[2] After detecting a link interruption, the slave device waits for the duration of the *Topology Change* timeout before forwarding packets between the 2 network segments.

Link Topology Requirements

Confirm that the following links are direct, without any other devices in between:

- The 2 links connecting the inner ports (2, 4) of each coupler pair in the respective primary and secondary rings.

This helps ensure that a link interruption is detected by the RCP devices.

Application Example for RCP Coupling

Loops during the configuration phase may lead to unintended equipment operation.

⚠ **WARNING**

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the RCP configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

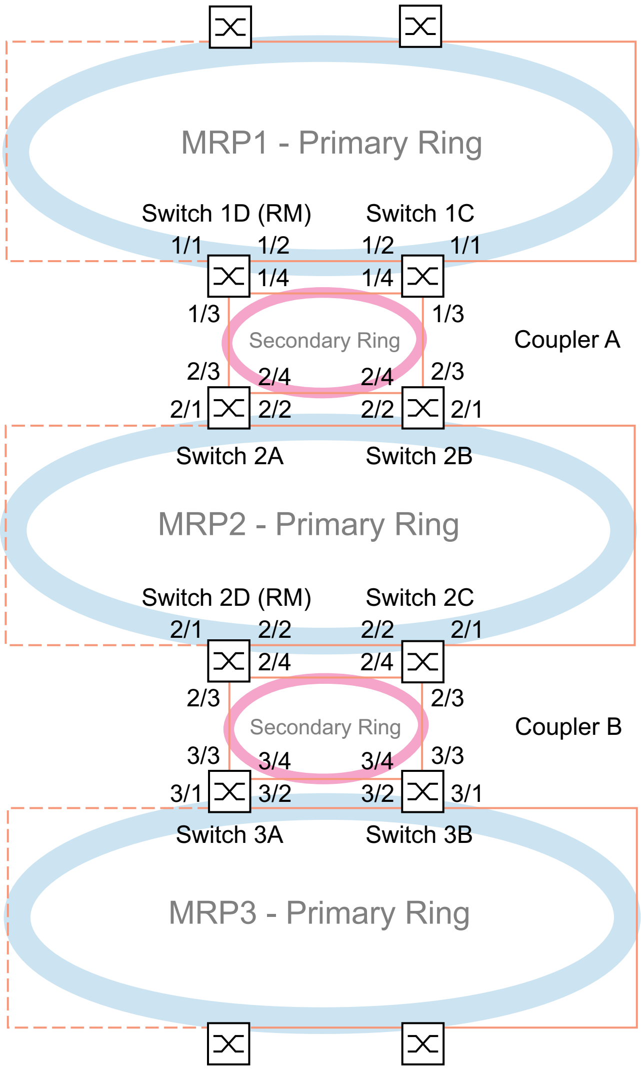
The Schneider Electric devices support the two-switch redundant coupling. You can use the RCP function to provide a network installed in a train for example. The network provides information for the passengers about the train location or the different stops on the line. The network can also include video surveillance.

The primary rings in the figure represent an MRP ring within each car. Each primary ring consists of 4 devices. See the following figure.

The secondary rings in the figure represent RSTP rings that automatically form when 2 cars are being coupled. Each secondary ring consists of 2 coupler pairs that are joined through their respective outer ports. In the figure, these device quadruples are called Coupler A and B.

To simplify the port configuration, the MRP ring ports and the RCP inner and outer ports are assigned the same port numbers on each switch. For example, on the switches 2A..2D, specify the ports ***2/1*** and ***2/2*** as MRP Ring ports, the ports ***2/4*** as RCP inner ports, and the ports ***2/3*** as RCP outer ports.

The following figure presents the Redundant Coupling Protocol Train Topology:



Ports ***x/1*** and ***x/2***: MRP ring ports
Ports ***x/3***: RCP outer ports
Ports ***x/4***: RCP inner ports

The following steps describe how to specify the parameters for the railway car represented by the MRP2 ring.

Set up the switches 2A..2C as an MRP *Ring Client* device. Set up only switch 2D as the MRP *Ring Manager* device. Set up the switches 2A and 2B as one RCP coupler pair and the switches 2C and 2D as the second coupler pair.

Disabling the RSTP Function on the MRP Ring Ports

MRP and RSTP do not work together. Therefore, deactivate the RSTP function on the RCP ports used in the MRP ring. In the example configuration, ports **x/1** and **x/2** are used for the MRP ring. Activate the RSTP function only on the RCP inner and outer ports used in the secondary ring. For example, activate the RSTP function on the ports **x/3** and **x/4**.

If you disable the MRP function, the device re-enables the RSTP function on the RCP ports used in the primary ring. In the example configuration, the device re-enables RSTP on ports **x/1** and **x/2**.

> **NOTE:** Substitute the port designation examples like **x/1** with the actual port numbers on your system. Depending on your device, the port designation may consist of only the port number.

Perform the following steps on the switches 2A..2D:

Step	Action
1	Navigate to the **Switching > L2-Redundancy > Spanning Tree > Port**, **CIST** tab.
2	In the default setting, the RSTP function is active on the ports. To deactivate the RSTP function on the MRP ring ports, clear the STP active checkboxes for ports **x/1** and **x/2**.
3	Navigate to **Switching > L2-Redundancy > Spanning Tree > Global**.
4	Enable the Spanning Tree function. Select the **On** radio button in the Operation frame.
5	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface x/1`	To change to the Interface Configuration mode of interface **x/1**.
`no spanning-tree mode`	To disable the Spanning Tree function on the port.
`exit`	To change to the Configuration mode.
`interface x/2`	To change to the Interface Configuration mode of interface **x/2**.
`no spanning-tree mode`	To disable the Spanning Tree function on the port.
`exit`	To change to the Configuration mode.
`spanning-tree operation`	To enable the Spanning Tree function.

Setting Up the MRP *Ring Manager* and *Ring Client* Devices

Set up the switches 2A..2C as an MRP *Ring Client* device. Set up only switch 2D as the MRP *Ring Manager* device (refer to Redundant Coupling Protocol Train Topology).

Set up the other switches in the rings as *Ring Client* devices. To do this, perform the following steps:

Step	Action
1	Navigate to **Switching > L2-Redundancy > MRP**.
2	Specify the first ring port in the Ring port 1 frame. From the Port drop-down list, select port **x/1**.
3	Specify the second ring port in the Ring port 2 frame. From the Port drop-down list, select port **x/2**.
4	On switch 2D only: To designate the device as the MRP *Ring Manager* device, enable the Ring manager function. For switches 2A..2C, use the default setting.
5	Enable the MRP function. Select the **On** radio button in the Operation frame.
6	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain add default-domain`	To add a MRP domain with the ID **default-domain**.
`mrp domain modify port primary x/1`	To specify port **x/1** as ring port **1**.
`mrp domain modify port secondary x/2`	To specify port **x/2** as ring port **2**.
`mrp domain modify mode manager`	On switch 2D only: To designate the device as the *Ring Manager* device. For switches 2A..2C, use the default setting.
`mrp domain modify operation enable`	To enable the MRP function.

Specifying the Ports for the RCP Coupler Pairs

Perform the following steps on the switches 2A..2D:

Step	Action
1	Navigate to **Switching > L2-Redundancy > FuseNet > RCP**.
2	Specify the Inner port in the Primary ring/network frame. Select port **x/2**.
3	Specify the Outer port in the Primary ring/network frame. Select port **x/1**.
4	Specify the Inner port in the Secondary ring/network frame. Select port **x/4**.
5	Specify the Outer port in the Secondary ring/network frame. Select port **x/3**.
6	Enable the RCP function. Select the **On** radio button in the Operation frame.
7	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`redundant-coupling port primary inner x/2`	To specify port **x/2** as the primary inner port.
`redundant-coupling port primary outer x/1`	To specify port **x/1** as the primary outer port.
`redundant-coupling port secondary inner x/4`	To specify port **x/4** as the secondary inner port.
`redundant-coupling port secondary outer x/3`	To specify port **x/3** as the secondary outer port.
`redundant-coupling operation`	To enable the RCP function in the device.

NOTE: The example leaves the roles of the coupler pair devices at the default value auto. The coupler pair devices then automatically select their roles as master or slave. When you want specific master or slave roles for a device pair, specify the roles explicitly.

Tracking

The tracking function allows monitoring of objects, such as the availability of an interface or reachability of a network.

Tracking can monitor the following objects:

- Link status of an interface (interface tracking)
- Result of logical connections of tracking entries (logic tracking)

An object can have the following statuses:

- up (OK)
- down (not OK)
- notReady (not enabled)

The definition of "up" and "down" depends on the type of the tracking object (for example interface tracking).

Tracking can forward the state changes of an object to the following applications:

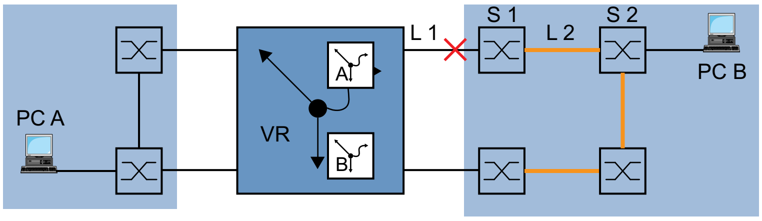
- Static routing
- Interface status

Interface Tracking

With interface tracking the device monitors the link status of:

- Physical ports
- Link Aggregation interfaces
- VLAN router interfaces

The following figure presents monitoring a line with interface tracking:



Ports/interfaces can have the following link statuses:

- interrupted physical link (link down)
- existing physical link (link up)

If the link to the participating ports is interrupted, a Link Aggregation interface has link status “down”.

If the link is interrupted from the physical ports/Link Aggregation interfaces that are members of the corresponding VLAN, the VLAN router interface has the link status “down”.

Setting a delay time allows the insertion of a delay before informing the application about an object status change.

If the physical link interruption remains for longer than the “link down delay” delay time, the interface tracking object has the status “down”.

When the physical link holds for longer than the “link up delay” delay time, the interface tracking object has the status “up”.

State on delivery: delay times = 0 seconds.

This means that in case where a status changes, the registered application is informed immediately.

You can set the “link down delay” and “link up delay” delay times independently of each other in the range from 0 to 255 seconds.

You can define an interface tracking object for each interface.

Logical Tracking

Logical tracking links multiple tracking objects so they can perform relatively complex monitoring tasks.

You can use logical tracking, for example, to monitor the link status for a network node to which redundant paths lead.

The device supports the following operators for a logical link:

- **and**
- **or**

A logical link combines up to two operands with one operator.

Logical tracking objects can have the following statuses:

- The result of the logical link is incorrect (**down**).
- The result of the logical link is correct (**up**).
- The monitoring of the tracking object is inactive (**notReady**).

When a logical link reports the status **down**, the device can select an alternative path.

Configuring the Tracking

You configure the tracking by creating tracking objects. To create a tracking object, perform the following steps:

- Enter the tracking object ID number (track ID).
- Select a tracking type, for example interface.
- Depending on the selected track type, enter additional options such as “port” or “link up delay” in the interface tracking.

  NOTE: The registration of applications (for example VRRP) to which the tracking function reports status changes is performed in the application itself.

Configuring Interface Tracking

To set up interface tracking on port **1/1** with a link down delay of **0** seconds and a link up delay of **3** seconds, perform the following steps:

Step	Action
1	Navigate to **Advanced > Tracking > Configuration**.
2	Click the ⊞ button. The dialog displays the Create window.
3	Select type. Enter the values you desire, for example: • Type: **interface** • Track ID: **11**
4	Click **OK**.
5	Properties Enter the values you desire, for example: • Port: **1/1** • Link up delay [s]: **3** • Link down delay [s]: **0**
6	To apply the settings, click the ✓ button.

Execute the following commands:

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><code>enable</code></td><td>To change to the Privileged EXEC mode.</td></tr>
<tr><td><code>configure</code></td><td>To change to the Configuration mode.</td></tr>
<tr><td><code>track add interface 11</code></td><td>To add a tracking object to the table.</td></tr>
<tr><td><code>track modify interface 11 ifnumber 1/1 link-up-delay 3 link-down-delay 0</code></td><td>To specify the parameters for this tracking object.</td></tr>
<tr><td><code>track enable interface 11</code></td><td>To activate the tracking object.</td></tr>
<tr><td colspan="2"><pre>
Tracking ID interface-11 created Target interface set to 1/1
  Link Up Delay for target interface set to 3 sec
  Link Down Delay for target interface set to 0 sec
Tracking ID 11 activated
</pre></td></tr>
<tr><td><code>exit</code></td><td>To change to the Privileged EXEC mode.</td></tr>
<tr><td><code>show track interface</code></td><td>To display the set-up tracking objects.</td></tr>
<tr><td colspan="2"><pre>
Name   If-Number Link-Up-Delay Link-Down-Delay State Active
-------- ---------- ------------- --------------- ----- ------
if-11   1/1   0   3   up   [x]
</pre></td></tr>
</table>

Interface Status Application

The interface status application allows control of the status of one or more interfaces based on the status changes of a tracking object.

For example:

- When the status of the tracking object changes to **down**, the status of the linked interfaces also changes to **down**.
- When the status of the tracking object changes to **up**, the status of the linked interfaces also changes to **up**.

The device allows the following interface types to link to a tracking object:

- Physical ports
- Link Aggregation interfaces

Special Conditions During Use

If you manually deactivate the linked interface, its status remains **down** even if the tracking object status changes to **up**.

The interface status application verifies the reason for disabling an interface. If the Auto-Disable function has disabled a linked interface, the interface status application does not enable this port again.

Example for the Interface Status Application

In the following example, the administrator links the tracking object **if-1** to interface **1/2**. When the status of the tracking object **if-1** changes, the interface status application changes the status of interface **1/2** accordingly. The prerequisite is that for interface **1/1**, a tracking object with Track name = **if-1** and Type =**interface** is set up. For details, refer to Configuring the Tracking, page 264.

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > Port**. The dialog displays the settings for the individual ports. You link a Link Aggregation interface in the **Switching > L2-Redundancy > Link Aggregation** dialog.
2	In the table row for interface **1/2**, **Track name** column, select the drop-down list, and click tracking object **if-1**.
3	To apply the settings, click the ✓ button.
4	Navigate to **Advanced > Tracking > Applications** dialog to display which applications are linked to the tracking objects.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface **1/2**.
`track if-status add if-1`	To link the tracking object **if-1** to interface **1/2**.
`show track application`	To verify the status of the applications.

```
Type         Track-Id   App-Name                                App-
Object-Name
----------   --------   --------------------------------------
---------------
interface           1   IntfState 1/1                           if-1
```

`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Operation Diagnosis

The device provides you with the following diagnostic tools:

- Sending SNMP traps
- Monitoring the Device Status
- Out-of-Band signaling using the signal contact
- Event counter at port level
- Detecting non-matching duplex modes
- Auto-Disable
- Displaying the SFP status
- Topology discovery
- Detecting IP address conflicts
- Detecting loops
- Help protect against layer 2 network loops
- Reports
- Monitoring data stream on a port (port mirroring)
- Syslog
- Event log
- Cause and action management during self test

Sending SNMP Traps

The device immediately reports unusual events that occur during normal operation to the network PC. This is done by messages called SNMP traps that bypass the polling procedure (“polling” means querying the data stations at regular intervals). SNMP traps allow you to react to unusual events.

Examples of such events are:

- Hardware reset
- Changes to the configuration
- Segmentation of a port

The device sends SNMP traps to various hosts to increase the transmission reliability for the messages. The unacknowledged SNMP trap message consists of a packet containing information about an unusual event.

The device sends SNMP traps to those hosts specified in the trap destination table. The device allows the setup of the trap destination table with the network PC using SNMP.

SNMP Traps for Configuration Activity

After you save a configuration in the memory, the device sends a **sa2ConfigurationSavedTrap**. This SNMP trap contains both the state variables of non-volatile memory (**NVM**) and external memory **ENVM**) indicating if the running configuration is in sync with the non-volatile memory, and with the external memory. You can also trigger this SNMP trap by transferring a configuration file onto the device, replacing the active saved configuration.

Furthermore, the device sends a **sa2ConfigurationChangedTrap**, whenever you change the local configuration, indicating a mismatch between the running and saved configuration.

SNMP Trap Setting

The device allows an SNMP trap as a reaction to specific events. Set up at least one trap destination that receives SNMP traps.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > Status Configuration > Alarms (Traps)**.
2	Click the + button. The dialog displays the Create window.
3	In the Name frame, specify the name that the device uses to identify itself as the source of the SNMP trap.
4	In the Address frame, specify the IP address of the trap destination to which the device sends the SNMP traps.
5	In the Active column, select the entries that the device takes into account when it sends SNMP traps.
6	To apply the settings, click the ✓ button.

For example, in the following dialogs you specify when the device triggers an SNMP trap:

- **Basic Settings > Port** dialog
- **Basic Settings > Power over Ethernet > Global** dialog
- **Network Security > Port Security** dialog
- **Switching > L2-Redundancy > Link Aggregation** dialog
- **Advanced > Tracking > Configuration** dialog
- **Diagnostics > Status Configuration > Device Status** dialog
- **Diagnostics > Status Configuration > Security Status** dialog
- **Diagnostics > Status Configuration > Signal Contact** dialog
- **Diagnostics > Status Configuration > MAC Notification** dialog
- **Diagnostics > System > IP Address Conflict Detection** dialog
- **Diagnostics > System > Selftest** dialog
- **Diagnostics > Ports > Port Monitor** dialog
- **Advanced > Digital IO Module** dialog

ICMP Messaging

The device allows the Internet Control Message Protocol (ICMP) for diagnostic applications, for example ping and trace route. The device also uses ICMP for time-to-live and discarding messages in which the device forwards an ICMP message back to the packet source device.

Use the ping network tool to test the path to a particular host across an IP network. The traceroute diagnostic tool displays paths and transit delays of packets across a network.

Monitoring the Device Status

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device to present its condition in graphic form.

The device displays its present status as **error** or **ok** in the Device status frame. The device determines this status from the individual monitoring results.

The device allows:

- Out-of-Band signaling using a signal contact
- Signal the changed device status by sending an SNMP trap
- Detect the device status in the **Basic Settings > System** dialog of the Graphical User Interface
- Query the device status in the Command Line Interface

The **Global** tab of the **Diagnostics > Status Configuration > Device Status** dialog allows the device to send a trap to the PC for the following events:

- Incorrect supply voltage
  - At least one of the 2 supply voltages is not operating
  - The internal supply voltage is not operating
- When you operate the device outside of the user-specified temperature threshold values
- Loss of the redundancy (when the device operates in the *Ring Manager* mode)
- The interruption of link connection(s)

  Set up at least one port for this feature. In the table of the **Port** tab, Propagate connection error column, you specify for which ports the device will propagate a link interruption to the device status. In the default setting, link connection monitoring is inactive.
- The removal of the external memory (**ENVM)**

  The configuration profile in the external memory (**ENVM)** does not match the settings in the device.

Select the corresponding entries to determine which events the device status includes.

NOTE: With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

Monitored Events

The following table describes the device status events:

Name	**Description**
Connection errors	Activate this function to monitor every port link event in which the Propagate connection error checkbox is selected.
Temperature	Activate this function to monitor if the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value.
External memory removed	Activate this function to monitor the presence of an external storage device.
External memory not in sync with NVM	The device monitors synchronization between the device settings and the configuration profile stored in the external memory (**ENVM)**.
Ring redundancy	When ring redundancy is present, activate this function to monitor.
Humidity	Activate this function to monitor when the humidity exceeds or falls below the specified threshold values.
Power supply	Activate this function to monitor the power supply.

Configuring the Device Status

Perform the following steps:

Step	Action
1	Navigate to the **Diagnostics > Status Configuration > Device Status**, **Global** tab.
2	For the parameters to be monitored, select the checkbox in the Monitor column.
3	To send an SNMP trap to the PC, activate the Send trap function in the Traps frame.
4	In the **Diagnostics > Status Configuration > Alarms (Traps)** dialog, add at least one trap destination that receives SNMP traps.
5	To apply the settings, click the ✓ button.
6	Navigate to **Basic Settings > System**.
7	To monitor the temperature, in the System data frame, you specify the temperature threshold values.
8	To monitor the humidity, in the System data frame, you specify the humidity threshold values.
9	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`device-status trap`	To send an SNMP trap when the device status changes.
`device-status monitor envm-not-in-sync`	To monitor the configuration profiles in the device and in the external memory (**ENVM**). The Device status changes to **error** in the following situations: • The configuration profile only exists in the device. • The configuration profile in the device differs from the configuration profile in the external memory (**ENVM**).
`device-status monitor envm-removal`	To monitor the active external memory (**ENVM**). When you remove the active external memory from the device, the value in the Device status frame changes to **error**.
`device-status monitor power-supply 1`	To monitor the power supply unit **1**. When the device has a detected power supply error, the value in the Device status frame changes to **error**.
`device-status monitor ring-redundancy`	To monitor the ring redundancy. The Device status changes to **error** in the following situations: • The device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve. • The device, as a ring participant, has detected an error in its ring redundancy settings.
`device-status monitor temperature`	To monitor the temperature in the device. When the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value, the value in the Device status frame changes to **error**.
`device-status monitor humidity`	To monitor the humidity in the device. When the humidity exceeds or falls below the specified threshold values, the value in the Device status frame changes to **error**.

To enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

Step	Action
1	Navigate to the **Diagnostics > Status Configuration > Device Status**, **Global** tab.
2	For the Connection errors parameter, select the checkbox in the Monitor column.
3	Navigate to the **Diagnostics > Status Configuration > Device Status**, **Port** tab.
4	For the Propagate connection error parameter, select the checkbox in the column of the ports to be monitored.
5	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`device-status monitor link-failure`	To monitor the ports/interfaces link. When the link interrupts on a monitored port/interface, the value in the Device status frame changes to **error**.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`device-status link-alarm`	To monitor the port/interface link. When the link interrupts on a monitored port/interface, the value in the Device status frame changes to **error**.

NOTE: The previous commands activate monitoring and trapping for supported components. When you want to activate or deactivate monitoring for individual components, you can find the corresponding syntax in the *Modicon MCSESM, MCSESP Series Managed Switch Command Line Interface User Guide* or in the help of the Command Line Interface console. To display the help in Command Line Interface, insert a question mark **?** and press the **Enter** key.

Displaying the Device Status

Perform the following steps:

Step	Action
1	Navigate to **Basic Settings > System**.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`show device-status all`	To display the device status and the setting for the device status determination.

Security Status

The Security Status provides an overview of the overall security of the device. Many processes aid in system visualization by recording the security status of the device and then presenting its condition in graphic form. The device displays the overall security status in the **Basic Settings > System** dialog, Security status frame.

In the **Global** tab of the **Diagnostics > Status Configuration > Security Status** dialog the device displays its present status as **error** or **ok** in the Security status frame. The device determines this status from the individual monitoring results.

The device allows:

- Out-of-Band signaling using a signal contact
- Signal the changed security status by sending an SNMP trap
- Detect the security status in the **Basic Settings > System** dialog of the Graphical User Interface
- Query the security status in the Command Line Interface

Monitored Events

Perform the following steps:

- Specify the events that the device monitors.
- For the corresponding parameter, select the checkbox in the Monitor column.

The following table describes security status events:

Name	Description
Password default settings unchanged	After installation change the passwords. When active and the default passwords remain unchanged, the device displays an alarm.
Min. password length shorter than 8	Create passwords more than 8 characters long. When active, the device monitors the Min. password length setting.
Password policy settings deactivated	The device monitors the settings located in the **Device Security > User Management** dialog for password policy requirements.
User account password policy check deactivated	The device monitors the settings of the Policy check checkbox. When Policy check is inactive, the device sends an SNMP trap.
Telnet server active	Activate this function to monitor when the Telnet function is active.
HTTP server active	Activate this function to monitor when the HTTP function is active.
SNMP unencrypted	Activate this function to monitor when the SNMPv1 or SNMPv2 function is active.
Access to System Monitor 1 through the serial interface possible	The device monitors if starting the System Monitor 1 through the serial connection is possible during the system startup.
Saving the configuration profile on the external memory possible	The device monitors the possibility to save settings to the external non-volatile memory.
Link interrupted on enabled device ports	The device monitors the link status of active ports.
Access with Ethernet Switch Configurator possible	Activate this function to monitor when the Ethernet Switch Configurator function has write access to the device.
Load unencrypted config from external memory	The device monitors the security settings for loading the configuration from the external non-volatile memory.
IEC 61850-MMS active	The device monitors the IEC 61850-MMS protocol activation setting.
Self-signed HTTPS certificate present	The device monitors the HTTPS server for self-generated digital certificates.
Modbus TCP active	The device monitors the Modbus TCP/IP protocol activation setting.

Configuring the Security Status

Perform the following steps:

Step	Action
1	Navigate to the **Diagnostics > Status Configuration > Security Status**, **Global** tab.
2	For the parameters to be monitored, select the checkbox in the Monitor column.
3	To send an SNMP trap to the PC, activate the Send trap function in the Traps frame.
4	To apply the settings, click the ✓ button.
5	In the **Diagnostics > Status Configuration > Alarms (Traps)** dialog, add at least one trap destination that receives SNMP traps.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`security-status monitor pwd-change`	To monitor the password for the locally set up user account **admin**. When the password for the **admin** user account is the default setting, the value in the Security status frame changes to **error**.
`security-status monitor pwd-min-length`	To monitor the value specified in the Min. password length policy. When the value for the Min. password length policy is less than **8**, the value in the Security status frame changes to **error**.
`security-status monitor pwd-policy-config`	To monitor the password policy settings. When the value for at least one of the following policies is specified as **0**, the value in the Security status frame changes to **error**. • Uppercase characters (min.) • Lowercase characters (min.) • Digits (min.) • Special characters (min.)
`security-status monitor pwd-policy-inactive`	To monitor the password policy settings. When the value for at least one of the following policies is specified as **0**, the value in the Security status frame changes to **error**.
`security-status monitor telnet-enabled`	To monitor the Telnet server. When you enable the Telnet server, the value in the Security status frame changes to **error**.
`security-status monitor http-enabled`	To monitor the HTTP server. When you enable the HTTP server, the value in the Security status frame changes to **error**.
`security-status monitor snmp-unsecure`	To monitor the SNMP server. When at least one of the following conditions applies, the value in the Security status frame changes to **error**: • The SNMPv1 function is enabled. • The SNMPv2 function is enabled. • The encryption for SNMPv3 is disabled. You enable the encryption in the **Device Security > User Management** dialog, in the **SNMP encryption type** field.
`security-status monitor sysmon-enabled`	To monitor the activation of the System Monitor 1 function in the device.
`security-status monitor extnvm-upd-enabled`	To monitor the activation of the external non-volatile memory update.
`security-status monitor iec61850-mms-enabled`	To monitor the IEC 61850-MMS function. When you enable the IEC 61850-MMS function, the value in the Security status frame changes to **error**.
`security-status trap`	To send an SNMP trap when the device status changes.

To enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

Step	Action
1	Navigate to the **Diagnostics > Status Configuration > Security Status**, **Global** tab.
2	For the Link interrupted on enabled device ports parameter, select the checkbox in the Monitor column.
3	To apply the settings, click the ✓ button.
4	Navigate to the **Diagnostics > Status Configuration > Device Status**, **Port** tab.
5	For the Link interrupted on enabled device ports parameter, select the checkbox in the column of the ports to be monitored.
6	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`security-status monitor no-link-enabled`	To monitor the link on active ports. When the link interrupts on an active port, the value in the Security status frame changes to **error**.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`security-status monitor no-link`	To monitor the link on interface/port **1**.

Displaying the Security Status

Perform the following step:

Step	Action
1	Navigate to **Basic Settings > System**.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`show security-status all`	To display the security status and the setting for the security status determination.

Out-of-Band Signaling

The device uses the signal contact to control external devices and monitor device functions. Function monitoring allows remote diagnostics.

The device reports the operating status using a break in the potential-free signal contact (relay contact, closed circuit) for the selected mode. The device monitors the following functions:

- Incorrect supply voltage
  - At least one of the 2 supply voltages is not operating
  - The internal supply voltage is not operating

- When you operate the device outside of the user-specified temperature threshold values
- When you operate the device outside of the user-specified humidity threshold values
- Events for ring redundancy:

  The device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve.

  The device, as a ring participant, has detected an error in its ring redundancy settings.

  In the default setting, ring redundancy monitoring is inactive.
- The interruption of link connection(s)

  Set up at least one port for this feature. In the Propagate connection error frame, you specify which ports the device signals for a link interruption. In the default setting, link monitoring is inactive.
- The removal of the external memory (**ENVM**)

  The configuration profile in the external memory (**ENVM**) does not match the settings in the device.

Select the corresponding entries to determine which events the device status includes.

NOTE: With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

Controlling the Signal Contact

With the **Manual setting** mode you control this signal contact remotely.

Application options:

- Simulation of an error detected during SPS error monitoring
- Remote control of a device using SNMP, such as switching on a camera

Perform the following steps:

Step	Action
1	Navigate to the **Diagnostics > Status Configuration > Signal Contact**, **Global** tab.
2	To control the signal contact manually, in the Configuration frame, select **Manual setting** from the Mode drop-down list.
3	Open the signal contact. Select the **open** radio button in the Configuration frame.
4	Close the signal contact. Select the **close** radio button in the Configuration frame.
5	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`signal-contact 1 mode manual`	To select the manual setting mode for signal contact **1**.
`signal-contact 1 state open`	To open signal contact **1**.
`signal-contact 1 state closed`	To close signal contact **1**.

Monitoring the Device and Security Statuses

In the **Configuration** field, you specify which events the signal contact indicates.

- **Device status**

  Using this setting the signal contact indicates the status of the parameters monitored in the **Diagnostics > Status Configuration > Device Status** dialog.

- **Security status**

  Using this setting the signal contact indicates the status of the parameters monitored in the **Diagnostics > Status Configuration > Security Status** dialog.

- **Device/Security status**

  Using this setting the signal contact indicates the status of the parameters monitored in the **Diagnostics > Status Configuration > Device Status** and the **Diagnostics > Status Configuration > Security Status** dialog.

Configuring the Operation Monitoring

Perform the following steps:

Step	Action
1	Navigate to the **Diagnostics > Status Configuration > Signal Contact**, **Global** tab.
2	To monitor the device functions using the signal contact, in the Configuration frame, specify the value **Monitoring correct operation** in the **Mode** field.
3	For the parameters to be monitored, select the checkbox in the Monitor column.
4	To send an SNMP trap to the PC, activate the Send trap function in the Traps frame.
5	To apply the settings, click the ✓ button.
6	In the **Diagnostics > Status Configuration > Alarms (Traps)** dialog, add at least one trap destination that receives SNMP traps.
7	To apply the settings, click the ✓ button.
8	You specify the temperature threshold values for the temperature monitoring in the **Basic Settings > System** dialog.
9	You specify the humidity threshold values for the humidity monitoring in the **Basic Settings > System** dialog.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`signal-contact 1 monitor temperature`	To monitor the temperature in the device. When the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value, the signal contact opens.
`signal-contact 1 monitor humidity`	To monitor the humidity in the device. When the humidity exceeds or falls below the specified threshold values, the signal contact opens.
`signal-contact 1 monitor ring-redundancy`	To monitor the ring redundancy. The signal contact opens in the following situations: • The device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve. • The device, as a ring participant, has detected an error in its ring redundancy settings.
`signal-contact 1 monitor link-failure`	To monitor the ports/interfaces link. When the link interrupts on a monitored port/interface, the signal contact opens.
`signal-contact 1 monitor envm-removal`	To monitor the active external memory (**ENVM**). When you remove the active external memory (**ENVM**) from the device, the signal contact opens.
`signal-contact 1 monitor envm-not-in-sync`	To monitor the configuration profiles in the device and in the external memory (**ENVM**). The signal contact opens in the following situations: • The configuration profile only exists in the device. • The configuration profile in the device differs from the configuration profile in the external memory (**ENVM**).
`signal-contact 1 monitor power-supply 1`	To monitor the power supply unit **1**. When the device has a detected power supply error, the signal contact opens.
`signal-contact 1 monitor module-removal 1`	To monitor module **1**. When you remove module **1** from the device, the signal contact opens.
`signal-contact 1 trap`	To send an SNMP trap when the status of the operation monitoring changes.
`no signal-contact 1 trap`	To disable the SNMP trap

To enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

Step	Action
1	In the Monitor column, activate the Link interrupted on enabled device ports function.
2	Navigate to the **Diagnostics > Status Configuration > Device Status**, **Port** tab.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`signal-contact 1 monitor link-failure`	To monitor the ports/interfaces link. When the link interrupts on a monitored port/interface, the signal contact opens.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`signal-contact 1 link-alarm`	To monitor the port/interface link. When the link interrupts on the port/interface, the signal contact opens.

Monitored Events

The following table describes device status events:

Name	Description
Connection errors	Activate this function to monitor every port link event in which the Propagate connection error checkbox is selected.
Temperature	Activate this function to monitor if the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value.
External memory removed	Activate this function to monitor the presence of an external storage device.
External memory not in sync with NVM	The device monitors synchronization between the device settings and the configuration profile stored in the external memory (**ENVM**).
Ring redundancy	When ring redundancy is present, activate this function to monitor.
Humidity	Activate this function to monitor when the humidity exceeds or falls below the specified threshold values.
Power supply	Activate this function to monitor the power supply.

Displaying the Signal Contact Status

The device gives you additional options for displaying the status of the signal contact:

- Display in the Graphical User Interface
- Query in the Command Line Interface

Perform the following step:

Step	Action
1	Navigate to **Basic Settings > System**. The Signal contact status frame displays the signal contact status and informs you about alarms that have been detected.

Execute the following commands:

Command	Description
`show signal-contact 1 all`	To display the settings for the specified signal contact.

Port Event Counter

The port statistics table assists network administrators in identifying potential network interruptions.

The packet counters add up the events sent and the events received. In the **Basic Settings > Restart** dialog, you can reset the event counters.

The following table presents event counters and examples.

Counter	Indication
Received fragments	• Non-functioning controller of the connected device • Electromagnetic interference in the transmission medium
CRC Error	• Non-functioning controller of the connected device • Electromagnetic interference in the transmission medium • Inoperable component in the network
Collisions	• Non-functioning controller of the connected device • Network over extended/lines too long • Collision or a detected error with a data packet

Perform the following steps:

Step	Action
1	To display the event counter, navigate to the **Basic Settings > Port**, **Statistics** tab.
2	To reset the counters, in the **Basic Settings > Restart** dialog, click **Clear port statistics**.

Detecting Non-Matching Duplex Modes

Potential detected issues occur when two ports directly connected to each other have mismatched duplex modes. These potential detected issues are difficult to detect. The automatic detection and reporting of this situation has the benefit of recognizing mismatched duplex modes before potential detected issue occur.

This situation arises from an incorrect configuration, for example, deactivation of the automatic configuration on the remote port.

A typical effect of this non-matching is that at a low data rate, the connection seems to be functioning, but at a greater bi-directional data stream level the local device records a lot of detected CRC errors, and the connection falls significantly below its nominal capacity.

The device allows detection of this situation and report it to the network PC. In the process, the device evaluates the detected error counters of the port in the context of the port settings.

Possible Causes of Port Error Events

The following table lists the duplex operating modes for TX ports, with possible detected errors. The meanings of terms used in the table are as follows:

- Duplex issue detected

  Mismatched duplex modes.
- EMI

  Electromagnetic interference.
- Network extension

  The network extension is too great, or too many cascading hubs.
- Collisions, *Late Collisions*

  In half-duplex mode, collisions mean normal operation.

  In full-duplex mode, no incrementation of the port counters for collisions or *Late Collisions*.
- CRC Error

  The device evaluates these detected errors as non-matching duplex modes in the manual full-duplex mode.

The following table presents evaluation of non-matching of the duplex mode:

Nb	**Automatic configuration**	**Duplex mode**	**Detected error events (≥ 10 after link up)**	**Duplex modes**	**Possible causes**
1	**selected**	Half-duplex	None	OK	–
2	**selected**	Half-duplex	Collisions	OK	–
3	**selected**	Half-duplex	Late Collisions	Duplex issue detected	Potential duplex issue, EMI, network extension
4	**selected**	Half-duplex	CRC Error	OK	EMI
5	**selected**	Full-duplex	None	OK	–
6	**selected**	Full-duplex	Collisions	OK	EMI
7	**selected**	Full-duplex	Late Collisions	OK	EMI
8	**selected**	Full-duplex	CRC Error	OK	EMI
9	**cleared**	Half-duplex	None	OK	–
10	**cleared**	Half-duplex	Collisions	OK	–
11	**cleared**	Half-duplex	Late Collisions	Duplex issue detected	Potential duplex issue, EMI, network extension
12	**cleared**	Half-duplex	CRC Error	OK	EMI
13	**cleared**	Full-duplex	None	OK	–
14	**cleared**	Full-duplex	Collisions	OK	EMI
15	**cleared**	Full-duplex	Late Collisions	OK	EMI
16	**cleared**	Full-duplex	CRC Error	Duplex issue detected	Potential duplex issue, EMI

Auto-Disable

The device can disable a port on various user-selectable events, such as a detected error or change of condition. Each of these events leads to the shutdown of the port. To recover the port, either clear the condition that caused the port shutdown or specify a timer to automatically re-enable the port.

If the device disables the port, the device no longer forwards data packets to and from that port. The port LED flashes green three times per cycle and indicates the reason for shutdown. The device also creates a log entry that records the causes of the deactivation. When you re-enable the port after a timeout using the Auto-Disable function, the device generates a log entry.

The Auto-Disable function provides a recovery function which automatically enables an auto-disabled port after a user-defined time. When this function enables a port, the device sends an SNMP trap with the port number, but without a value for the Reason parameter.

The Auto-Disable function serves the following purposes:

- Helps the network administrator in port analysis.
- Helps reduce the likelihood that the port will cause network instability.

The Auto-Disable function is available for the following functions:

- Link flap (Port Monitor function)
- CRC/Fragments (Port Monitor function)
- Duplex Mismatch detection (Port Monitor function)
- DHCP Snooping
- Dynamic ARP Inspection
- Spanning Tree
- Port Security
- Overload detection (Port Monitor function)
- Link speed/Duplex mode detection (Port Monitor function)

If the interface status application disables the port because the associated tracking object changes its status to **down**, the Auto-Disable function does not automatically enable the port.

In the following example, you configure the device to disable a port when violations of the threshold values occur in the **Diagnostics > Ports > Port Monitor** dialog on the **CRC/Fragments** tab, and then automatically re-enable a port.

Perform the following steps:

Step	Action
1	Navigate to the **Diagnostics > Ports > Port Monitor**, **CRC/Fragments** tab.
2	Verify that the threshold values specified in the table concur to your preferences for port **1/1**.
3	Navigate to the **Diagnostics > Ports > Port Monitor**, **Global** tab.
4	Enable the Port Monitor function. Select the **On** radio button in the Operation frame.
5	To allow the device to disable the port due to detected errors, select the checkbox in the CRC/Fragments on column for port **1/1**.
6	In the Action column you can choose how the device reacts to detected errors. In this example, the device disables port **1/1** for threshold value violations and then automatically re-enables the port. • To allow the device to disable and automatically re-enable the port, select the value **auto-disable** and set up the Auto-Disable function. The value **auto-disable** only works in conjunction with the Auto-Disable function. The device can also disable a port without auto re-enabling. • To allow the device to disable the port only, select the value **disable port**. • To manually re-enable a disabled port, select the table row of the port and click the 🗑 button. When you set up the Auto-Disable function, the value **disable port** also automatically re-enables the port.
7	Navigate to the **Diagnostics > Ports > Port Monitor**, **Auto-disable** tab.
8	To allow the device to auto re-enable the port after it was disabled due to detected threshold value violations, select the checkbox in the CRC error column.
9	Navigate to the **Diagnostics > Ports > Port Monitor**, **Port** tab.
10	Specify the delay time as 120 s in the Reset timer [s] column for the ports you want to enable. **NOTE: Reset** allows the port to be enabled before the time specified in the Reset timer [s] column has expired.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`port-monitor condition crc-fragments count 2000`	To specify the CRC-Fragment counter to 2000 parts per million.
`port-monitor condition crc-fragments interval 15`	To set the measure interval to 15 seconds for CRC-Fragment detection.
`auto-disable timer 120`	To specify the waiting period of **120** seconds, after which the Auto-disable function re-enables the port.
`exit`	To change to the Configuration mode.
`auto-disable reason crc-error`	To activate the auto-disable CRC function.
`port-monitor condition crc-fragments mode`	To activate the CRC-Fragments condition to trigger an action.
`port-monitor operation`	To activate the Port Monitor function.

When the device disables a port due to threshold value violations, the device allows the following commands to manually reset the disabled port.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`auto-disable reset`	To let you enable the port before the time has expired.

Displaying the SFP Status

The SFP status display allows a view of the SFP module connections and their properties. The properties include:

- Module type
- Serial number of media module
- Temperature in ° C
- Transmission power in mW
- Receive power in mW

Perform the following step:

Step	Action
1	Navigate to **Diagnostics > Ports > SFP**

Topology Discovery

IEEE 802.1AB defines the Link Layer Discovery Protocol (LLDP). LLDP allows automatic detection of the LAN network topology.

Devices with LLDP active:

- Broadcast their connection and management information to neighboring devices on the shared LAN. When the receiving device has its LLDP function active, evaluation of the devices occur.
- Receive connection and management information from neighbor devices on the shared LAN, provided these adjacent devices also have LLDP active.
- Build a management information database and object definitions for storing information about adjacent devices with LLDP active.

As the main element, the connection information contains an exact, unique identifier for the connection end point: MAC (Service Access Point). This is made up of a device identifier which is unique on the entire network and a unique port identifier for this device:

- Chassis identifier (its MAC address)
- Port identifier (its port-MAC address)
- Description of port
- System name
- System description
- Supported system capabilities
- Active system capabilities
- Interface ID of the management address
- VLAN-ID of the port
- Auto-negotiation status on the port
- Medium, half/full-duplex setting and port speed setting
- Information about the VLANs installed in the device (VLAN-ID and VLAN name, irrespective of whether the port is a VLAN participant).

A network PC can call up this information from devices with activated LLDP. This information allows the network PC to map the topology of the network.

Non-LLDP-capable devices normally block the special multicast LLDP IEEE MAC address used for information exchange. Non-LLDP-capable devices therefore discard LLDP packets. If you position a non-LLDP-capable device between 2 LLDP-capable devices, the non-LLDP-capable device prohibits information exchanges between the 2 LLDP-capable devices.

The Management Information Base (MIB) for a device with LLDP capability holds the LLDP information in the lldp MIB and in the private SA2-LLDP-EXT-HM-MIB and SA2-LLDP-MIB.

Displaying the Topology Discovery Results

Display the topology of the network. To do this, perform the following step:

Step	Action
1	Navigate to the **Diagnostics > LLDP > Topology Discovery**, **LLDP** tab.

When you use a port to connect several devices, for example through a hub, the table contains a line for each connected device.

If you connect the port to devices with the topology discovery function active, the devices exchange LLDP Data Units (LLDPDU) and the topology table displays these neighboring devices.

When a port connects only devices without an active topology discovery, the table contains a line for this port to represent the connected devices. This line contains the number of connected devices.

The MAC address table (forwarding database) contains MAC addresses of devices that are not shown in the topology table for clarity.

LLDP-Med

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices. Endpoints include devices such as IP phones, or other Voice over IP (VoIP) devices or servers and network devices such as switches. It specifically provides support for VoIP applications. LLDP-MED provides this support using an additional set of common type-length-value

(TLV) advertisement messages, for capabilities discovery, network policy, Power over Ethernet, inventory management and location information.

The device supports the following TLV messages:

- Capabilities TLV

  Lets the LLDP-MED endpoints determine the capabilities that the connected device supports and what capabilities the device has enabled.

- Network policy TLV

  Lets both network connectivity devices and endpoints advertise VLAN configurations and associated attributes for the specific application on that port. For example, the device notifies a phone of the VLAN number. The phone connects to a switch, obtain its VLAN number, and then starts communicating with the call control.

LLDP-MED provides the following functions:

- Network policy discovery, including VLAN ID, 802.1p priority and DSCP (Differentiated Services Code Point)
- Device location and topology discovery based on LAN-level MAC/port information
- Endpoint move detection notification, from network connectivity device to the associated VoIP management application
- Extended device identification for inventory management
- Identification of endpoint network connectivity capabilities, for example, multi-port IP Phone with embedded switch or bridge capability
- Application level interactions with the Link Layer Discovery Protocol (LLDP) elements to provide timely startup of LLDP to support rapid availability of an Emergency Call Service
- Applicability of LLDP-MED to Wireless LAN environments, support for Voice over Wireless LAN

Detecting Loops

Loops in the network cause connection interruptions or data loss. This also applies to temporary loops. The automatic detection and reporting of this situation allows faster detection and easier diagnosis.

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the ring configuration individually.
- Complete the configuration of the other devices of the ring configuration before you connect the redundant lines.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

An incorrect configuration causes loops, for example, deactivating Spanning Tree.

The device allows the detection of the effects typically caused by loops and report this situation automatically to the network PC. You have the option here to specify the magnitude of the loop effects that trigger the device to send a report.

BPDU frames sent from the *Designated port* and received on either a different port of the same device or the same port within a short time, is a typical effect of a loop.

To verify if the device has detected a loop, perform the following steps:

Step	Action
1	Navigate to the **Switching > L2-Redundancy > Spanning Tree > Port**, **CIST** tab.
2	Verify the value in the **Port state** and **Port role** fields. If the **Port state** field displays the value **discarding** and the **Port role** field displays the value **backup**, the port is in a loop status.

Or:

Step	Action
1	Navigate to the **Switching > L2-Redundancy > Spanning Tree > Port**, **Guards** tab.
2	Verify the value in the Loop state column. If the field displays the value **true**, the port is in a loop status.

Avoid Layer 2 Network Loops

The device has a Loop Protection function.

A network loop can lead to a standstill of the network due to overload. A possible reason is the continuous duplication of data packets due to a misconfiguration. The cause could be, for example, an improperly connected cable or an incorrect setting in the device.

For example, a layer 2 network loop can occur in the following cases, if no redundancy protocols are active:

- Two ports of the same device are directly connected to each other.
- More than one active connection is established between two devices.

Loops during the configuration phase may lead to unintended equipment operation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Set up each device of the layer 2 network individually.
- Complete the configuration of the other devices of the layer 2 network before you connect the redundant lines.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The Loop Protection function is enabled in every device:

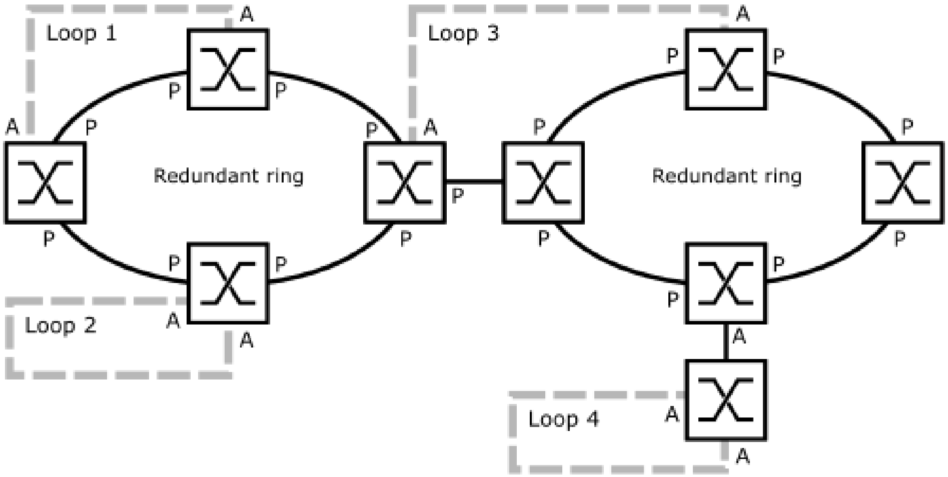
- **A**: *Active mode*

  Ports that are intended to connect end devices operate in the active mode. The device evaluates and sends *loop detection* packets on these ports.
- **P**: *Passive mode*

  Ports which belong to the redundant rings operate in the passive mode. The device only evaluates *loop detection* packets on these ports.
- **Loop 1**..**Loop 4**

  Unintentionally set-up layer 2 network loops.

The following figure presents examples for unintended layer 2 network loops:



Assigning the Loop Protection Settings to the Ports

For each *active* and each *passive* port, assign the settings of the Loop Protection function.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > Loop Protection**
2	In the Global frame, **Transmit interval** field, adjust the value, if necessary.
3	In the Global frame, **Receive threshold** field, adjust the value, if necessary.
4	In the Mode column, specify the behavior of the Loop Protection function on the port: • **active** For ports that are intended to connect end devices. • **passive** For ports that belong to the redundant rings.
5	In the Action column, specify the value all. When the device detects a layer 2 loop on this port, it sends a trap and disables the port using the Auto-Disable function. If necessary, adjust the value.
6	In the Active column, select the checkbox.
7	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`loop-protection tx-interval 5`	To specify the transmit interval, if necessary.
`loop-protection rx-threshold 1`	To specify the receive threshold value, if necessary.
`interface 1/1`	To change to the Interface mode. Example: port ***1/1***.
`loop-protection mode active`	To specify the mode `active` for ports that are intended to connect end devices.
`loop-protection mode passive`	To specify the mode `passive` for ports which belong to the redundant rings.
`loop-protection action all`	To specify the action that the device performs when it detects a layer 2 network loop on this port.
`loop-protection operation`	To activate the Loop Protection function on the port.
`exit`	To change to the Configuration mode.

Activating the Auto-Disable Function

After you assigned the Loop Protection settings to the ports, activate the Auto-Disable function.

Perform the following steps:

Step	Action
1	In the Configuration frame, select the Auto-disable checkbox.
2	To apply the settings, click the ✓ button.

Execute the following command:

Command	Description
`loop-protection auto-disable`	To activate the Auto-Disable function.

Enabling the Loop Protection Function in the Device

When finished, enable the Loop Protection function in the device.

Perform the following steps:

Step	Action
1	Select the **On** radio button in the Operation frame.
2	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`loop-protection operation`	To enable the Loop Protection function in the device.

Guidelines for Redundant Ports

Depending on the Loop Protection settings, the device disables ports using the Auto-Disable function when the device detects a layer 2 network loop.

If any redundancy function is active on a port, do not activate the active mode on this port. Otherwise, port shutdowns on redundant network paths can be the result. In the example above these are the ports which belong to the redundant rings.

Verify that a redundant network path is available as backup media. The device changes to the redundant path in case of the outage of the primary path.

The following settings help avoid port shutdowns on redundant network paths:

- Disable the Loop Protection function on redundant ports.

  or

- Enable the passive mode on redundant ports.

The Loop Protection function and the Spanning Tree function have an effect on each other. The following steps help avoid unexpected behavior of the device:

- Disable the Spanning Tree function on the port on which you want to enable the Loop Protection function. See the **Switching > L2-Redundancy > Spanning Tree > Port** dialog, STP active column.
- Disable the Spanning Tree function on the connected port of each connected device. See the **Switching > L2-Redundancy > Spanning Tree** dialog.

Using the Email Notification Function

The device allows communication of events that have occurred. Prerequisite is that a mail server is available through the network on which the device transfers the emails.

To set up the device to send emails, perform the steps in the following chapters:

- Specifying the Sender Address, page 291
- Specifying the Triggering Events, page 292
- Specifying the Recipients, page 293
- Specifying the Mail Server, page 294
- Enabling/Disabling the Email Notification Function, page 295
- Sending a Test Email, page 295

Specifying the Sender Address

The sender address is the email address that indicates the device which sent the email.

Change the preset value. To do this, perform the following steps:

Step	Action
1	Navigate to **Diagnostics > Email Notification > Global**
2	In the Sender frame, change the value in the **Email address** field. Add a valid email address.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email from-addr <user@doma.in>`	To change the sender address.

Specifying the Triggering Events

The device differentiates between the following severities:

Severity	Description
emergency	Device not ready for operation
alert	Immediate user intervention required
critical	Critical error detected
error	Error detected
warning	Advisory
notice	Significant, normal status
informational	Informal message
debug	Debug message

You have the option of specifying the events of which the device informs you. For this, assign the desired minimum severity to the notification levels of the device.

The device informs the recipients as follows:

- Notification urgent

  When an event of the severity assigned or more severe occurs, the device sends an email immediately.
- Notification non-urgent
  - When an event of the severity assigned or more severe occurs, the device logs the event in a buffer.
  - The device sends an email with the log file periodically or if the buffer is full.
  - When an event of a lower severity occurs, the device does not log this event.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics** > **Email Notification** > **Global**
2	In the Notification urgent frame, you specify the settings for emails which the device sends immediately. • In the **Severity** field, you specify the minimum severity. • In the **Subject** field, you specify the subject of the email.
3	In the Notification non-urgent frame, you specify the settings for emails which the device sends periodically. • In the **Severity** field, you specify the minimum severity. • In the **Subject** field, you specify the subject of the email.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email severity immediate <level>`	To specify the minimum severity for events for which the device sends an email immediately.
`logging email severity periodic <level>`	To specify the minimum severity for events for which the device sends an email periodically.
`logging email subject add <immediate | periodic> TEXT`	To add a subject line with the content **TEXT**.

Changing the Sending Interval

The device allows the specification of the interval in which it sends emails with the log file. The default setting is **30** minutes.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > Email Notification > Global** .
2	In the Notification non-urgent frame, you specify the settings for emails which the device sends periodically. Change the value in the **Sending interval [min]** field to change the interval.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email duration <30..1440>`	To specify the interval at which the device sends emails with log file.

Specifying the Recipients

The device allows up to 10 recipients.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > Email Notification > Recipients**.
2	To add a table row, click the + button.
3	In the Notification type column, specify if the device sends the emails to this recipient immediately or periodically.
4	In the Email address column, specify the email address of the recipient.
5	In the Active column, select the checkbox.
6	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email to-addr add <1..10> addr <user@doma.in> msgtype <immediately | periodically>`	To specify the recipient with the email address **user@doma.in**. The device manages the settings in memory **1..10**.

Specifying the Email Server

The device supports encrypted and unencrypted connections to the mail server.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > Email Notification > Mail Server**.
2	To add a table row, click the ⊞ button.
3	In the IP address column, specify the IP address or the DNS name of the server.
4	In the Encryption column, specify the protocol which encrypts the connection between the device and the mail server.
5	When the mail server uses a port other than the defined port, specify the TCP port in the Destination TCP port column.
6	When the mail server requests an authentication, in the User name and Password columns, specify the account credentials which the device uses to authenticate on the mail server.
7	In the Description column, enter a meaningful name for the mail server.
8	In the Active column, select the checkbox.
9	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email mail-server add <1..5> addr <IP ADDRESS> [security <none|tlsv1>] [username <USER NAME>] [password <PASSWORD>] [port <1..65535>]`	To specify the mail server with the IP address **IP ADDRESS**. The device manages the settings in memory **1..5**.

Enabling/Disabling the Email Notification Function

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > Email Notification > Global**.
2	Enable the Email Notification function. Select the **On** radio button in the Operation frame.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email operation`	To enable the sending of emails.
`no logging email operation`	To disable the sending of emails.

Sending a Test Email

The device allows verification of the settings by sending a test email.

Prerequisite:

- The email settings are completely specified.
- The Email Notification function is enabled.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > Email Notification > Mail Server**.
2	Click the ✉ button. The dialog displays the Connection test window.
3	From the Recipient drop-down list, select to which recipients the device sends the test email.
4	In the **Message text** field, specify the text of the test email.
5	Click **OK** to send the test email.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email test msgtype <urgent|non-urgent> TEXT`	To send an email with the content **TEXT** to the recipients.

When you do not see any message for detected errors and the recipients obtain the email, the device settings are correct.

Reports

The following lists reports and buttons available for diagnostics:

- System Log file

  The device logs device-internal events in the System Log file.
- Audit Trail

  Logs successful commands and user comments. The file also includes SNMP logging.
- Persistent Logging

  When the external memory is present, the device saves log entries in a file in the external memory. These files remain available even after powering off the device. The maximum size, maximum number of retainable files, and the severity of logged events are configurable. After obtaining the user-defined maximum size or maximum number of retainable files, the device archives the entries and starts a new file. The device deletes the oldest file and renames the other files to maintain the number of files set up. To review these files, use the Command Line Interface or copy them to an external server for future reference.
- Download support information

  This button allows system information to download as a ZIP archive.

In service situations, these reports provide the technician with the necessary information.

Global Settings

Using this dialog you enable or disable where the device sends reports, for example, to a Console, a syslog server, or a connection to the Command Line Interface. You also set at which severity level the device writes events into the reports.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > Report > Global**.
2	To send a report to the console, specify the desired level in the Console logging frame, **Severity** field.
3	Enable the Console logging function. Select the **On** radio button in the Console logging frame.
4	To apply the settings, click the ✓ button.

The device buffers logged events in 2 separate storage areas so that the device keeps log entries for urgent events. Specify the minimum severity for events that the device logs to the buffered storage area with a greater priority.

Perform the following steps:

Step	Action
1	To send events to the buffer, specify the desired level in the Buffered logging frame, **Severity** field.
2	To apply the settings, click the ✓ button.

When you activate the logging of SNMP requests, the device logs the requests as events in the syslog. The Log SNMP get request function logs user requests for device configuration information. The Log SNMP set request function logs device setup events. Specify the minimum level for events that the device logs in the syslog.

Perform the following steps:

Step	Action
1	Enable the Log SNMP get request function for the device to send SNMP Read requests as events to the syslog server. Select the **On** radio button in the SNMP logging frame.
2	Enable the Log SNMP set request function for the device to send SNMP Write requests as events to the syslog server. Select the **On** radio button in the SNMP logging frame.
3	Choose the desired severity level for the get and set requests.
4	To apply the settings, click the ✓ button.

When active, the device logs configuration changes made using the Command Line Interface, to the audit trail. This feature is based on IEEE 1686 for Substation Intelligent Electronic Devices.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics** > **Report** > **Global**.
2	Enable the CLI logging function. Select the **On** radio button in the CLI logging frame.
3	To apply the settings, click the ✓ button.

The device allows the following system information to be saved in one ZIP file on your PC:

- audittrail.html
- defaultconfig.xml
- script
- runningconfig.xml
- supportinfo.html
- systeminfo.html
- systemlog.html

The device names the ZIP archive automatically in the format <IP_address>_<system_name>.zip.

Perform the following steps:

Step	Action
1	Click the ⬇ button. After a while, you can download the ZIP archive.
2	Select the directory in which you want to save the support information.
3	Click **OK**.

Syslog

The device allows messages about device internal events to one or more syslog servers (up to 8). Additionally, you also include SNMP requests to the device as events in the syslog.

> **NOTE:** To display the logged events, navigate to **Diagnostics > Report > Audit Trail** dialog or **Diagnostics > Report > System Log** dialog.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics** > **Syslog**.
2	To add a table row, click the + button.
3	In the IP address column, enter the IP address or *Hostname* of the syslog server. You can specify a valid IPv4 or IPv6 address for the syslog server.
4	In the Destination UDP port column, specify the TCP or UDP port on which the syslog server expects the log entries.
5	In the Min. severity column, specify the minimum severity level that an event requires for the device to send a log entry to this syslog server.
6	Select the checkbox in the Active column.
7	Enable the Syslog function. Select the **On** radio button in the Operation frame.
8	To apply the settings, click the ✓ button.

In the SNMP logging frame, set up the following settings for SNMP read and write requests.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics** > **Report** > **Global**.
2	Enable the Log SNMP get request function for the device to send SNMP Read requests as events to the syslog server. Select the **On** radio button in the SNMP logging frame.
3	Enable the Log SNMP set request function for the device to send SNMP Write requests as events to the syslog server. Select the **On** radio button in the SNMP logging frame.
4	Choose the desired severity level for the get and set requests.
5	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging host add 1 addr 10.0.1.159 severity 3`	To add a recipient in the syslog servers list. In this example, the severity value `3` indicates that the messages are classified with an **error** severity level.
`logging host add 2 addr 2001::1 severity 4`	To add an IPv6 recipient in the syslog servers list. In this example, the severity value `4` indicates that the messages are classified with a **warning** severity level.
`logging syslog operation`	To enable the Syslog function.
`exit`	To change to the Privileged EXEC mode.
`show logging host`	To display the syslog host settings.

```
No.    Server IP       Port   Max. Severity   Type        Status
-----  --------------  -----  --------------  ----------  -------
1      10.0.1.159      514    error           systemlog   active
2      2001::1         514    warning         systemlog   active
```

`configure`	To change to the Configuration mode.
`logging snmp-requests get operation`	To log the reception of *SNMP Get requests*.
`logging snmp-requests get severity 5`	The value **5** specifies the severity level of the event that the device logs when it receives an *SNMP Get request*. The value **5** means **notice**.
`logging snmp-requests set operation`	To log the reception of *SNMP Set requests*.
`logging snmp-requests set severity 5`	The value **5** specifies the severity level of the event that the device logs when it receives an *SNMP Set request*. The value **5** means **notice**.
`exit`	To change to the Privileged EXEC mode.
`show logging snmp`	To display the SNMP logging settings.

```
Log SNMP GET requests               : enabled
Log SNMP GET severity               : notice
Log SNMP SET requests               : enabled
Log SNMP SET severity               : notice
```

System Log

The device allows a System Log file of the system events. The table in the **Diagnostics > Report > System Log** dialog lists the logged events.

You have the following options:

- View and Refresh the System Log File, page 299
- Searching for Content, page 300
- Downloading a Copy of the System Log File, page 300
- Clearing the System Log File on the Device, page 301

You have the option to also send the logged events to one or more syslog servers.

View and Refresh the System Log File

The device continuously logs events in the System Log file. The display of events in the Graphical User Interface does not update automatically. If the dialog is already open for a while, refresh the display to also display the recently logged events.

Perform the following step:

Step	Action
1	Refresh the display of the System Log file in the Graphical User Interface. To do this, click the ⟳ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`show logging buffered`	To display the buffered log entries.

Searching for Content

The device continuously logs events in the System Log file. After a while, the file may contain a large number of events.

Perform the following step:

Step	Action
	• Look for a keyword in the System Log file. To do this, use the search function of your web browser.

Execute the following command:

Command	Description
`show logging buffered <filter>`	To display the buffered log entries. You can enter keywords for the severity level, digits, or ranges, separated by a comma. Example: `emergency,alert-error,4,5-6`

Downloading a Copy of the System Log File

The device continuously logs events in the System Log file. After a while, the file may contain many events. In the Graphical User Interface, you can download a copy of the System Log file to analyze the logged events on your computer. Using the Command Line Interface, you can save a copy of the System Log file in the external memory (**ENVM**) or on a remote server.

Perform the following steps:

Step	Action
1	Download a copy of the System Log file onto your computer. To do this, click the ⤓ button.
2	The web browser saves the file on the computer according to its download settings. If necessary, select the file location.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`copy eventlog buffered envm EXAMPLE`	To save a copy of the System Log file with filename `EXAMPLE` in the external memory (**ENVM**).
`copy eventlog buffered remote ftp://1.2.3.4/EXAMPLE`	To save a copy of the System Log file with filename `EXAMPLE` on a remote server.

Clearing the System Log File on the Device

The device continuously logs events in the System Log file. After a while, the file may contain many events. If you are no longer verifying logged events, you can clear the System Log file in the device.

Perform the following step:

Step	Action
1	Delete the content of the System Log file. To do this, click the 🗑 button.

Execute the following command:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`clear logging buffered`	To clear the log file.

Syslog over TLS

The Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating computer applications.

When initiating a connection with a syslog server, using a TLS handshake, the device validates the digital certificate received from the server. For this purpose, you transfer the digital certificate from a remote server or from the external memory (**ENVM**) onto the device. Verify that the specified IP address or DNS name of the server matches the `Common Name` or `Subject Alternative Name` information in the digital certificate.

The device sends the TLS encrypted syslog messages over the TCP port specified in the Destination UDP port column.

> **NOTE:** To establish an encrypted connection using a digital certificate, verify that the `Common Name` or `Subject Alternative Name` information in the digital certificate that you have transferred onto the device matches the IP address or DNS name of the server.

Application Example for the Syslog Function

The given example describes the configuration of the Syslog function. By following these steps, the device allows TLS encrypted syslog messages to be sent over the TCP port specified in the Destination UDP port column.

The syslog messages that are sent from a device to a syslog server can pass through untrusted networks. To set up a syslog-over-TLS server, transfer the digital certificate onto the device. Use only digital certificates signed by a Certification Authority (CA).

> **NOTE:** For the changes to take effect after transferring a digital certificate or a CRL into the device, disable and re-enable the Syslog function. See the Operation frame.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > Syslog**.
2	Initiate a data connection with the syslog servers. Select the **On** radio button in the Operation frame.
3	To apply the settings, click the ✓ button. The device validates the digital certificate received. The device also authenticates the server and starts sending syslog messages.
4	Transfer the digital certificate from the remote server or from the external memory (**ENVM**) onto the device.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging host add 1 addr 192.168.3.215`	To add index **1** to the syslog server with IPv4 address **192.168.3.215**.
`logging host add 2 addr 2001::1`	To add index **2** to the syslog server with IPv6 address **2001::1.**
`logging host modify 1 port 6512 type systemlog`	To specify the port number **6512** and logging the events in the system log.
`logging host modify 1 transport tls`	To specify the type of transmission as **tls**.
`logging host modify 1 severity informational`	To specify the type of event to log into the system log as **informational**.
`exit`	To change to the Privileged EXEC mode.
`copy syslogcacert evmm`	To transfer the digital certificates from the external memory (**ENVM**) onto the device.
`show logging host`	To display the syslog host settings.

Audit Trail

The **Diagnostics > Report > Audit Trail** dialog contains system information and changes to the device settings performed through the Command Line Interface and SNMP. In the case of a change in the device settings, the dialog displays Who changed What and When.

The **Diagnostics > Syslog** dialog allows up to eight syslog servers to which the device sends Audit Trails.

The following list contains log events:

- Changes to configuration parameters
- Commands (except `show` commands) using the Command Line Interface
- Command `logging audit-trail <string>` using the Command Line Interface which logs the comment
- Automatic changes to the System Time
- Watchdog events
- Locking a user after several unsuccessful login attempts
- User login, either locally or remote, using the Command Line Interface
- Manual, user-initiated, logout
- Timed logout after a user-defined period of inactivity in the Command Line Interface
- File transfer operation including a device software update
- Configuration changes using Ethernet Switch Configurator
- Automatic configuration or device software updates using the external memory
- Blocked access to the device management due to invalid login
- Rebooting
- Opening and closing SNMP over HTTPS tunnels
- Detected power interruption

Network Analysis with TCPdump

Tcpdump is a packet-sniffing UNIX utility used by network administrators to monitor and analyze the data stream on a network. A couple of reasons for sniffing data streams on a network are to verify connectivity between hosts or to analyze the data stream traversing the network.

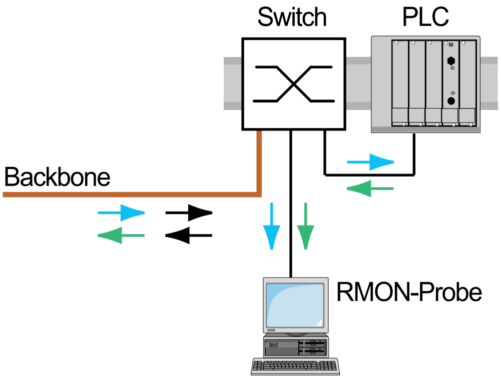
TCPDump in the device provides the possibility to decode or capture packets received and transmitted by the controller. This function is available using the `debug` command. For further information on the TCPDump function, see the “Command Line Interface” reference manual.

Monitoring the Data Stream with Port Mirroring

The Port Mirroring function allows data packets from physical source ports be copied to be copied to a physical destination port. Port Mirroring is defined as Switched Port Analyzer (SPAN).

You monitor the data packets on the source ports in the sending and receiving directions with a management tool connected on the destination port, for example an *RMON probe*. The function has no effect on the data stream running on the source ports.

The following figure presents an application example of a port-mirroring setup



On the destination port, the device only forwards the data packets copied from the source ports.

Before you switch on the Port Mirroring function, select the checkbox Allow management to access the device management through the destination port. The device allows users access to the device management through the destination port without interrupting the active Port Mirroring session.

> **NOTE:** The device duplicates multicasts, broadcasts and undefined unicasts on the destination port.
> The VLAN settings on the destination port remain unchanged. Prerequisite for access to the device management on the destination port is that the destination port is a member of the device management VLAN.

Enabling the Port Mirroring Function

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > Ports > Port Mirroring**.
2	Specify the source ports. Select the checkbox in the Enabled column for the relevant ports.
3	Specify the destination port. In the Destination port frame, select the desired port from the Primary port drop-down list. The drop-down list only displays available ports. Ports that are already specified as source ports are unavailable.
4	When needed, specify a second destination port. In the Destination port frame, select the desired port from the Secondary port drop-down list. The prerequisite is that you have already specified the primary destination port.
5	To access the device management through the destination port: In the Destination port frame, select the Allow management checkbox.
6	To apply the settings, click the ✓ button.

To deactivate the Port Mirroring function and restore the default settings, click the 🗑 button.

Monitoring Data Streams with RSPAN

RSPAN (Remote Switched Port Analyzer) extends the concept of Switched Port Analyzer (SPAN), which is also called Port Mirroring.

In contrast to SPAN, which operates on a single switch device, RSPAN uses a topology of 2 or more RSPAN-enabled devices. This allows the data stream at a location other than directly at the source to be analyzed.

Purpose

RSPAN allows data packets from selected locations in a network to be collected and the mirrored data packets at a convenient location to be monitored.

The data packets are collected by one or more devices acting in the *source role*. These *source devices* collect data packets from selectable *source ports*. A *source device* can have several *source ports*.

Each RSPAN-enabled device receives and forwards the mirrored data packets on a specified RSPAN VLAN to the final destination. This includes optional devices in an *intermediate role*, also called *intermediate devices*.

Finally, a device in the *destination role*, called *destination device*, sends the mirrored data packets to its local *destination port*. An analyzer tool, usually a dedicated computer, can then monitor or analyze the mirrored data packets at a convenient, for example, central location.

RSPAN key aspects are:

- Topology

  An RSPAN topology consists of 2 or more RSPAN-enabled devices.

  For details, refer to RSPAN Topologies, page 305.

- VLAN

  The RSPAN VLAN transfers the mirrored data packets between RSPAN-enabled devices.

  For details, refer to RSPAN VLAN Properties, page 308.

- Roles

  RSPAN roles are specific roles for the devices in an RSPAN topology.

  For details, refer to RSPAN Device Roles, page 308.

- Uplinks

  RSPAN uplinks can be separate uplinks or shared with normal uplinks.

  For details, refer to RSPAN Uplinks, page 310.

RSPAN Topologies

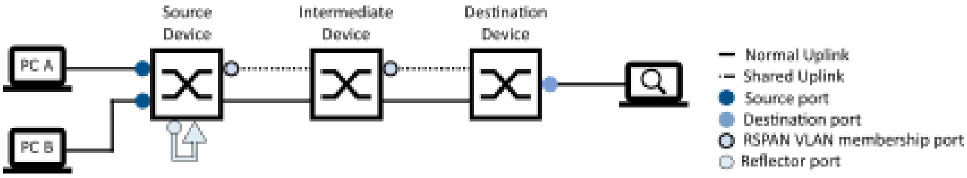
RSPAN topologies and the consequential locations of the devices in RSPAN roles can be:

- Line Topology, page 305
- Tree Topology, page 306
- Ring Topology, page 307

Line Topology

An RSPAN line topology is a line structure, superimposed on the existing network. The underlying network may have a more generalized topology, for example, a tree topology.

The following figure presents an example of a line topology, using a *reflector port* (with separate uplinks):



A line topology is a simple topology, where only one *source* and one *destination* device are required, and *intermediate devices* are optional:

- One *source device*

  The *source device* is located at one end of the line, at the data sources to be mirrored.
- One *destination device*

  The *destination device* is located at the other end of the line, near the analyzer tool.
- Optional *intermediate devices*

  The *intermediate devices* are located in the middle of the line, between the *source device* and the *destination device*. You can connect the *source device* directly to the *destination device*, if your situation allows.

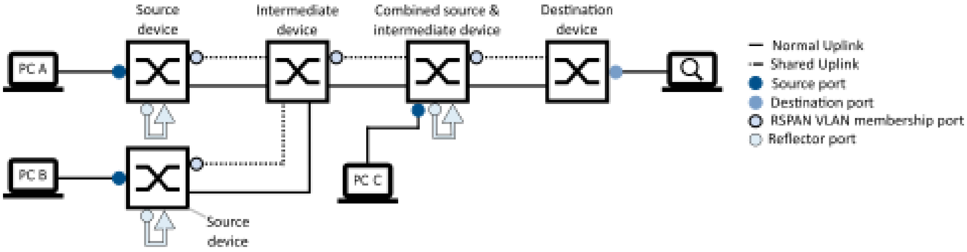
The graphics show separate uplinks for RSPAN and non-RSPAN data packets.

You can also create shared uplinks. For this, you use the normal (non-RSPAN) uplinks also for RSPAN. To create shared uplinks, select the existing, non-RSPAN uplink ports as RSPAN ports.

Tree Topology

An RSPAN tree topology is a tree structure, superimposed on the existing network. The underlying network may have a more generalized topology, for example, a mesh topology.

The following figure presents an example of a complex tree topology, using *reflector ports* (with separate uplinks):



A tree topology consists of:

- 2 or more *source devices*

  The *source devices* are located at the leaves of the tree, at the data sources to be mirrored.
- One *destination device*

  The *destination device* is located at the root of the tree, near the analyzer tool.
- Optional *intermediate devices*

  The *intermediate devices are* located as nodes in the middle of the tree, between the *source device* and the *destination device*. You can connect the *source devices* directly to the *destination device*, if your situation allows.

Tree topology subtypes:

- Simple tree topology:

  A simple tree topology requires only one *destination* and several *source devices*. *Intermediate* devices are optional, and the topology requires no *combined source/intermediate devices*.

- Complex tree topology:

  A complex tree topology requires additionally one or more *combined source/intermediate devices*. For details, refer to Combined Source/Intermediate Role, page 310.

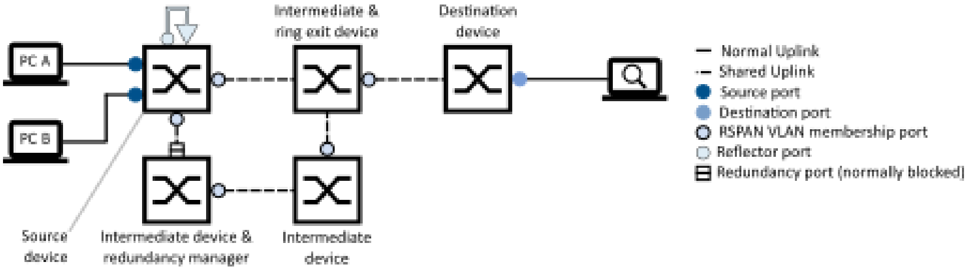
The graphics show separate uplinks for RSPAN and non-RSPAN data packets.

You can also create shared uplinks. For this, you use the normal (non-RSPAN) uplinks also for RSPAN. To create shared uplinks, select the existing, non-RSPAN uplink ports as RSPAN ports.

Ring Topology

An RSPAN ring topology is a ring structure, superimposed on the existing network. The underlying network may have a more generalized topology, for example, coupled rings.

The following figure presents an example of a simple ring topology based on an existing redundant ring (with shared links):


Intermediate & ring exit device
Destination device
PC A
PC B
Source device
Intermediate device & redundancy manager
Intermediate device
Normal Uplink
Shared Uplink
Source port
Destination port
RSPAN VLAN membership port
Reflector port
Redundancy port (normally blocked)

A ring topology consists of:

- In the ring:
  - One *source device*

    The *source device* is located in the ring, at the data sources to be mirrored.

    The *source device* has 2 *destination ports* and needs a *reflector port*.
  - One or more *intermediate devices*

    One of the *intermediate devices* forwards the RSPAN data packets out of the ring. In the following, this device is called the ring exit device.

    The other *intermediate devices* are located in the ring, between the *source device* and the ring exit device.

    The *intermediate devices* have one RSPAN VLAN membership port each.
- Outside the ring:
  - One *destination device*

    The *destination device is* located outside the ring, near the analyzer tool.

    You can connect the ring exit device directly to the *destination device*, if your situation allows.
  - Optional *intermediate devices*

    These optional *intermediate devices* connect the ring exit device to the *destination device*.

When setting up the RSPAN VLAN membership ports of the *intermediate devices* in the ring, consider the following data packet stream scenarios to the ring exit device:

- The regular RSPAN data packet stream, with the ring intact and the redundancy port blocked
- The alternate RSPAN data packet stream, with the ring interrupted and the redundancy port active

  NOTE: The special case where the *source device* is also the ring exit device, is considered a line topology.

Ring topology subtypes:

- Simple ring topology

  A simple ring topology requires only *source, intermediate*, and *destination* devices, but no *combined source/intermediate devices*.
- Complex ring topology

  A complex ring topology additionally requires one or more *combined source/ intermediate devices*. For details, refer to Combined Source/Intermediate Role, page 310.

RSPAN VLAN Properties

The flow of mirrored data packets within the RSPAN VLAN is unidirectional towards the *destination port* of the *destination device*. Consequently, the devices disable source MAC address learning in the RSPAN VLAN and flood the mirrored data packets within the RSPAN VLAN. Because of this, only the RSPAN *destination ports* have to be set up as a members of the RSPAN VLAN.

In contrast, ports receiving RSPAN data packets are not members of the RSPAN VLAN.

The *destination ports* of a *source device* send RSPAN data packets in the following way:

- The device adds a single RSPAN VLAN tag to untagged source data packets.
- The device inserts an additional RSPAN VLAN tag into tagged source data packets. This results in double VLAN tagged data packets. The device inserts the RSPAN VLAN tag as the first VLAN tag (outer tag, EtherType 0x8100).

RSPAN Device Roles

The possible RSPAN roles in a topology have the following names, instances, functions, and specific settings:

- Destination Role, page 308
- Source Role, page 309
- Intermediate Role, page 309
- Combined Source/Intermediate Role, page 310

Destination Role

The *destination role* is mandatory and requires exactly one instance in an RSPAN topology.

- A *destination device* has its *destination port* connected to an analyzer tool.
- In a tree topology, the *destination device* is the root of the tree.
- In a redundant ring, place the *destination device* outside the ring. This makes the setup of the *destination device* easier. For details, refer to Use of Underlying Redundancy Protocols, page 311.

The *destination device* receives the mirrored data packets on the RSPAN VLAN, either directly from the *source devices*, or indirectly through *intermediate devices*.

The *destination port* has the following properties:

- On a *destination device*, you can set up exactly one *destination port*.
- The *destination port* usually keeps the RSPAN VLAN tag when sending a data packet to the analyzer tool.
- If desired, the *destination port* can also strip the RSPAN VLAN tag.
  - For a tagged source data packet, this restores the original VLAN tag.
  - For an untagged source data packet, this restores the original untagged data packet.

Source Role

The *source role* is mandatory and needs one or more instances in an RSPAN topology. A *source device* only collects data packets from *source ports*. A pure *source device* has no ports that receive RSPAN data packets from other devices. For a *combined source/intermediate device*, refer to Combined Source/ Intermediate Role, page 310.

The *source device* collects the data packets it receives or sends on its selected local *source ports*. The device forwards the mirrored data packets on the RSPAN VLAN, either directly to the *destination device*, or to an *intermediate device*.

- The *source device* requires a *reflector port*. For details, refer to Reflector Port on a Source Device, page 311.
- To set up a *source device* with 2 *destination port*s, set up a *reflector port*. A possible use case is a *source device* in a ring redundancy topology. For details, refer to Use of Underlying Redundancy Protocols, page 311.
- The *destination port* adds the RSPAN VLAN tag when sending the data packet.

Intermediate Role

Depending on the RSPAN topology, the *intermediate role* has the following number of instances:

Topology	Subtype	Intermediate role instances
Line	–	Optional
Tree	Simple	Optional
	Complex	Optional
Ring	Simple	One or more
	Complex	One or more

For an *intermediate device*, you only need to set up the RSPAN VLAN. The device does not need any specific RSPAN settings.

An *intermediate device* has one or more ports that receive RSPAN data packets but no *source ports*.

An *intermediate device* receives the mirrored data packets on the RSPAN VLAN and forwards the mirrored data packets. When sending the data packets, the *destination port* keeps the RSPAN VLAN tag.

NOTE: Verify that the ports receiving the mirrored data packets are not members of the RSPAN VLAN.

Combined Source/Intermediate Role

Depending on the RSPAN topology, the *combined source/intermediate device* has the following number of instances:

Topology	Subtype	Combined source/intermediate role instances
Line	–	–
Tree	Simple	None
	Complex	One or more
Ring	Simple	None
	Complex	One or more

A *combined source/intermediate device* integrates the functions of a *source device* with that of an *intermediate device*:

- The *combined source/intermediate device* is located at the nodes of the topology tree, like *intermediate devices*.
- The device collects the data packets it receives or sends on its selected local *source ports*.
- The device forwards the mirrored data packets, either directly to the *destination device*, or to another *intermediate device* towards the *destination device*. When sending the data packets, the *destination port* adds the RSPAN VLAN tag to the source data packets.
- The device additionally receives mirrored data packets on one or more additional ports, either directly from one or more *source devices*, or from one or more other *intermediate devices*.
- The device forwards the mirrored data packets, either directly to the *destination device*, or to another *intermediate device* towards the *destination device*. When sending the data packets, the *destination port* keeps the RSPAN VLAN tag in the received mirrored data packets.
- The device requires specific *source device* settings in addition to the RSPAN VLAN settings of an *intermediate device*.
- The device needs a *reflector port*. For details, refer to *Reflector port* on a *source device*, page 311.
- To set up the device with 2 *destination ports*, use a *reflector port*. A possible use case is a *source device* in a ring redundancy topology. For details, refer to Use of Underlying Redundancy Protocols, page 311.

RSPAN Uplinks

For a shared RSPAN uplink, the *source device* or *intermediate device* send the mirrored data packets over an existing, normal uplink.

- You do not need to connect an additional cable.
- A shared uplink is necessary if you want to use the device as a *source device* or *intermediate device* in a ring redundancy topology.
- If the combined data rate of the RSPAN and non-RSPAN data packets exceeds the bandwidth of the shared uplink, RSPAN data packets and non-RSPAN data packets may affect each other. For details, refer to Packet Prioritization, page 313.

For a separate RSPAN uplink, the *source device* or *intermediate device* send the mirrored data packets over a separate connection different from the existing uplink.

- This requires an extra cable connection.
- A separate RSPAN uplink provides an exclusive path for RSPAN data packets. Consequently, the non-RSPAN data packets on their uplink are unaffected by the RSPAN data packets on the separate uplink.

For both uplink types, the RSPAN ports may require individual Spanning Tree settings. For details, refer to Use of Underlying Redundancy Protocols, page 311.

Reflector port on a *source device*

The *reflector port* in a *source device* has a special function without a physical connection. The *reflector port* internally receives the mirrored data packets and reflects (mirrors) them into the RSPAN VLAN instead of sending them. This way, the *reflector port* transforms the function of local Switched Port Analyzer (SPAN), or *Port Mirroring*, into the remote function, RSPAN.

A *source device* needs a *reflector port*.

You use a *reflector port* to set up a *source device* with 2 *destination port*s. A possible use case is a *source device* in a ring redundancy topology. For details, refer to Use of Underlying Redundancy Protocols, page 311.

NOTE: A setup, where the reflector port has a link, is unsupported.

Use of Underlying Redundancy Protocols

You can use RSPAN in combination with the following redundancy protocols:

- Ring Redundancy, page 311
- Link Aggregation, page 312
- Spanning Tree, page 312

Ring Redundancy

RSPAN-enabled devices can forward RSPAN data packets over an underlying ring redundancy topology. Each ring connection serves as an RSPAN uplink between the *source device* and the directly connected *intermediate devices*, as well as between the other *intermediate devices*. This creates a redundant, shared RSPAN uplink.

A ring topology requires shared uplinks. The participating devices transmit the RSPAN data packets together with the other packets over their ring ports.

NOTE: The RSPAN roles are independent of the ring redundancy roles like *ring switch* and *ring manager*. However, there are guidelines in which the ring redundancy participant should be used as an *RSPAN source device*.

Planning RSPAN device roles and their setup in a redundant ring:

- Place the *destination device* outside the ring.

  This makes the setup of the *destination device* easier.
- If possible, use the one of the following *ring redundancy devices* as the RSPAN *source device*:
  - The *ring manager*
  - The *ring switch* connected to the blocked port of the *ring manager*

  This minimizes the flooding of mirrored data packets into paths not leading to the ring exit device, because the *ring manager* blocks one of these paths in the regular case.
- If you cannot use one of the above mentioned ring redundancy devices as the *source device*, flooding of mirrored data packets into paths not leading to the ring exit device is inevitable.

  Weigh up the advantages and disadvantages for your specific use case.
- If you plan a complex ring topology, you need at least one *combined source/ intermediate device* in addition to the *source device*. The same guidelines used for a simple ring topology apply when deciding which devices in the ring should act as source devices and which should act as combined source and intermediate devices.
- On the *source device*, set up both ring ports as *destination ports*.

  Use a *reflector port*.
- On the *intermediate devices* in the ring:
  - Determine the device that sends the mirrored data packets out of the ring.

    In the following, this device is called the ring exit device.
  - For the ring exit device, set up the port leading out of the ring as an RSPAN VLAN member.
  - For the other *intermediate devices* on the path to the ring exit device, set up the ring ports connected to the next *intermediate device* or the ring exit device as an RSPAN VLAN member. Consider both data packet stream scenarios: with the ring intact and with the ring interrupted.

Link Aggregation

The devices can forward RSPAN data packets over *Link Aggregation Group* (*LAG*) interfaces on the path from the *source devices* to the *destination device*, including the optional *intermediate devices*.

The *destination port* of the *destination device* needs to be a physical port.

Spanning Tree

For shared RSPAN uplinks based on a mesh topology with *Spanning Tree* (*STP*, *RSTP*, or *MSTP*), RSPAN requires no further *Spanning Tree* settings.

If you use separate RSPAN uplinks, deactivate the Spanning Tree function on the ports for the separate RSPAN uplinks.

For shared RSPAN uplinks based on a mesh topology with *MSTP*: Verify that the RSPAN topology matches the underlying *MSTP* topology for the RSPAN VLAN ID.

If you want RSPAN to use the redundant paths provided by *Spanning Tree*, consider setting up a RSPAN topology similar to a ring topology. This means:

- The *source device* may require 2 or more *destination ports* and then require a *reflector port*.
- The *intermediate devices* may require 2 or more RSPAN VLAN membership ports.

In the above case, the use of redundant RSPAN paths will result in the mirrored data packets being flooded into paths that lead to the *destination device*, but these paths are blocked by the redundancy protocol in the regular case. Weigh up the advantages and disadvantages for your specific use case.

Packet Prioritization

The *source device* sends the mirrored data packets with the fixed *CoS priority* of **0 (best effort)** in the VLAN tag.

If the combined data rate of the RSPAN and non-RSPAN data packets exceeds the bandwidth of the shared uplink, RSPAN data packets and non-RSPAN data packets may affect each other.

If you cannot tolerate a loss of non-RSPAN data packets and cannot solve this situation by other means, consider VLAN-tagging your non-RSPAN data packets and assign a *CoS priority* of **2 (excellent effort)** or greater to minimize the impact of RSPAN data packets on non-RSPAN data packets.

Starting Point for the Example

The network administrator wants to monitor specific data packets using a network analyzer tool located at a central location in the network. The options for setting up RSPAN devices in an existing network are illustrated below.

Boundary conditions:

- Device 1 collects the data packets from PC 1 on port **1/2**.
- The analyzer tool, which data accepts packets with a single or a double VLAN tag, is connected to device 3, port **3/3**.
- The devices 1 and 3 are connected by device 2. The RSPAN topology therefore is a simple line.
- For a possible separate uplink, the devices 1, 2 and 3 have unused ports available and a physical network connection is available between the devices 1 and 2, as well between the devices 2 and 3.
- The devices in the RSPAN topology are RSPAN-capable.

Setup options chosen by the network administrator:

- Separate or shared RSPAN uplinks are both possible and will be determined later.
- The RSPAN VLAN ID for the example is 30.
- Use PC 2 to set up RSPAN in the devices.

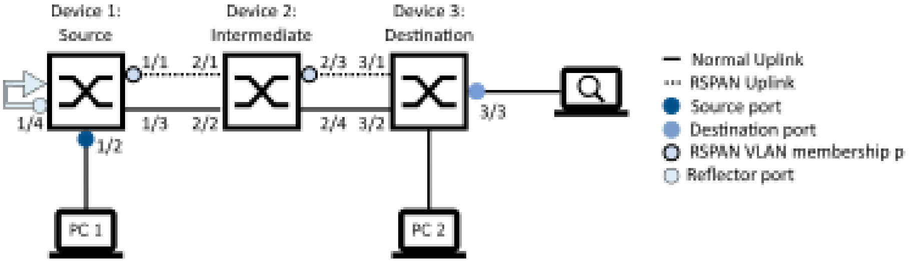
RSPAN data rate and connection bandwidth:

- For separate RSPAN uplinks:
  - Depending on the data rate of the RSPAN data packets and the bandwidth of the RSPAN connections, the device may drop some RSPAN data packets.
- For shared RSPAN uplinks:
  - Depending on the combined data rate of RSPAN and non-RSPAN data packets and the bandwidth of the shared connections, RSPAN and non-RSPAN data packets may affect one another.
- To address this, use connections with sufficient bandwidth, for example, Gigabit ports, LAG interfaces, or a combination thereof.

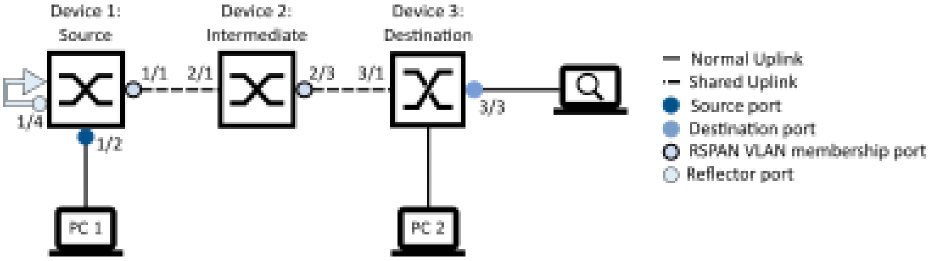
Example: RSPAN with a *reflector port*

In the following examples, you set up a simple RSPAN line topology, using a *reflector port* on the *source device*. There are 2 options, either with separate or with shared uplinks.

The following figure presents RSPAN in a line topology, using a *reflector port* (with separate uplinks):



The following figure presents RSPAN in a line topology, using a *reflector port* (with shared uplinks):



The work steps are the same for both options. The only difference is which ports make up the existing uplink for non-RSPAN packets.

- For a separate uplink, the existing uplink for non-RSPAN packets connects ports 1/3 and 2/2 and ports 2/4 and 3/2 respectively. The work steps will create a separate uplink for RSPAN packets after you physically connect the respective RSPAN ports.
- For a shared uplink, the existing uplink for non-RSPAN packets connects ports 1/1 and 2/1 and ports 2/3 and 3/1 respectively. The work steps will then create a shared uplink for RSPAN packets and non-RSPAN packets.

Setting Up Device 1 as the *source device*

Perform the following steps:

Step	Action
1	Navigate to **Switching** **>** **VLAN** **>** **Configuration**.
2	Add the RSPAN VLAN: • Click the + button. The dialog displays the Create window. • In the **VLAN ID** field, specify the value **30**. • Click **OK**. • In the VLAN **30** table row, RSPAN VLAN column, select the checkbox.
3	Specify the port connected to the *intermediate device*. In the VLAN **30** table row, column of port **1/1**, select **T** from the drop-down list.
4	To apply the settings, click the ✓ button.
5	Navigate to **Diagnostics** **>** **Ports** **>** **RSPAN**.
6	Specify the *source role*. In the Role frame, select **Source switch** from the drop-down list.
7	Specify the reflector port. In the Reflector port frame, select port **1/4** from the Reflector port drop-down list.
8	Specify the RSPAN VLAN ID. In the RSPAN frame, RSPAN Destination **VLAN ID** field, specify the value **30**.
9	Specify the Source port. In the row of port **1/2**, Active column, select the checkbox.
10	Specify the type of the data packets to be mirrored. In the row of port **1/2**, Type column, select the **txrx** item from the drop-down list.
11	Enable the function. In the Operation frame, select the **On** radio button.
12	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 30`	To add VLAN **30**.
`remote-vlan 30`	To specify VLAN **30** as the RSPAN VLAN ID.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of the *destination port*, interface **1/1**.
`vlan participation include 30`	To make port **1/1** a member in the RSPAN VLAN **30**.
`vlan tagging 30`	To send tagged data packets for the RSPAN VLAN **30**.
`exit`	To change to the Configuration mode.
`monitor session 1 source interface 1/2 operation enable`	To add port **1/2** as a *source port* to session **1**.
`monitor session 1 source interface 1/2 direction txrx`	To specify the type of the data packets to be mirrored on port **1/2** as **txrx** in session **1**.
`monitor session 1 remote-vlan 30 reflector-port 1/4`	To add VLAN **30** as the RSPAN VLAN, and to add port **1/4** as the *reflector port* to session **1**.
`monitor session 1 mode enable`	To activate the remote port mirroring session **1**.
`exit`	To change to the Privileged EXEC mode.

Setting Up Device 2 as the *intermediate device*

Perform the following steps:

Step	Action
1	Navigate to **Switching > VLAN > Configuration**.
2	Add the RSPAN VLAN: • Click the + button. The dialog displays the Create window. • In the **VLAN ID** field, specify the value **30**. • Click **OK**. • In the VLAN **30** table row, RSPAN VLAN column, select the checkbox.
3	Specify the port connected to the *destination device*. In the VLAN **30** table row, column of port **2/3**, select **T** from the drop-down list.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 30`	To add VLAN **30**.
`remote-vlan 30`	To specify VLAN **30** as the RSPAN VLAN ID.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 2/3`	To change to the Interface Configuration mode of the *destination port*, interface **2/3**.
`vlan participation include 30`	To make port **2/3** a member in the RSPAN VLAN **30**.
`vlan tagging 30`	To send tagged data packets for the RSPAN VLAN **30**.
`exit`	To change to the Configuration mode.

Setting Up Device 3 as the *destination device*

Perform the following steps:

Step	Action
1	Navigate to **Switching > VLAN > Configuration**.
2	Add the RSPAN VLAN: • Click the + button. The dialog displays the Create window. • In the **VLAN ID** field, specify the value **30**. • Click **OK**. • In the VLAN **30** table row, RSPAN VLAN column, select the checkbox.
3	To apply the settings, click the ✓ button.
4	Navigate to **Diagnostics > Ports > RSPAN**.
5	Specify the *destination role*. In the Role frame, select **Destination switch** from the drop-down list.
6	Specify the RSPAN VLAN. In the RSPAN frame, RSPAN Source **VLAN ID** field, specify the value **30**.
7	Specify the *destination port*. In the Destination port frame, select port **3/3** from the Destination port drop-down list.
8	Enable the function. In the Operation frame, select the **On** radio button.
9	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 30`	To add VLAN **30**.
`remote-vlan 30`	To specify VLAN **30** as the RSPAN VLAN ID.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`monitor session 1 destination interface 3/3`	To add port **3/3** as the *destination port* to session **1**.
`monitor session 1 source remote-vlan 30`	To add VLAN **30** as the RSPAN VLAN to session **1**.
`monitor session 1 mode enable`	To activate the remote port mirroring session **1**.
`exit`	To change to the Privileged EXEC mode.

Self-Test

The device verifies its assets during the system startup and occasionally thereafter. The device verifies system task availability or termination and the available amount of memory. Furthermore, the device verifies for application functionality and any hardware degradation in the chip set.

If the device detects a loss in integrity, the device responds to the degradation with a user-defined action. The following categories are available for configuration:

- **task**

  Action to be taken in case a task is unsuccessful.
- **resource**

  Action to be taken due to the lack of resources.
- **software**

  Action taken for loss of software integrity; for example, code segment checksum or access violations.
- **hardware**

  Action taken due to hardware degradation

Set up each category to produce an action in case the device detects a loss in integrity. The following actions are available for configuration:

- **log only**

  This action writes a message to the logging file.
- **send trap**

  Sends an SNMP trap to the trap destination.
- **reboot**

  If activated, a detected error in the category will cause the device to reboot.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > System > Selftest**.
2	In the Action column, specify the action to perform for a cause.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`selftest action task log-only`	To send a message to the event log when a task is unsuccessful.
`selftest action resource send-trap`	To send an SNMP trap when there are insufficient resources.
`selftest action software send-trap`	To send an SNMP trap when the software integrity has been lost.
`selftest action hardware reboot`	To reboot the device when hardware degradation is detected.

Disabling these functions allows a decrease of the time required to restart the device after a cold start. You find these options in the **Diagnostics > System > Selftest** dialog, Configuration frame.

- RAM test checkbox

  Activates/deactivates RAM self-test during a cold start.
- SysMon1 is available checkbox

  Activates/deactivates the option to start the System Monitor 1 during system startup.
  - **selected** (default setting)

    During system startup, the boot menu will display the System Monitor 1 item. The prerequisite is that the PC is connected to the device through the serial connection.

    To start the System Monitor 1, set the device to the Recovery Mode, refer to Access to Device Management, page 33.
  - **cleared**

    During system startup, the boot menu will not display the System Monitor 1 item.

    No one can start the System Monitor 1.
- Load default config on error checkbox

  Activates/deactivates the loading of the default device configuration in case no readable configuration is available during the system startup.

The following settings **block your access to the device permanently** in case the device does not detect any readable configuration profile at system startup.

- The SysMon1 is available checkbox is cleared.
- The Load default config on error checkbox is cleared.

This is the case, for example, when the password of the configuration profile that you are loading differs from the password set in the device. To have the device unlocked again, contact your sales partner.

Execute the following commands:

Command	Description
`selftest ramtest`	To activate RAM self-test on cold start.
`no selftest ramtest`	To deactivate RAM self-test.
`selftest system-monitor`	To activate the option to start the System Monitor 1. During system startup, the boot menu will display the System Monitor 1 item.
`no selftest system-monitor`	To deactivate the option to start the System Monitor 1. During system startup, the boot menu will not display the System Monitor 1 item.
`show selftest action`	To display the actions to be taken in the event of device degradation.

`Cause     Action`
`--------- ----------`
`task      reboot`
`resource  reboot`
`software  reboot`
`hardware  reboot`	

`show selftest settings`	To display the selftest settings.

`Selftest settings`
`-----------------`
`Test RAM on cold start......................enabled`
`System Monitor 1............................enabled`
`Boot default configuration on error.........enabled`	

Copper Cable Test

Use this function to verify a copper cable attached to a port for a short or open circuit. The test interrupts the data stream, when in progress, on this port.

The table displays the state and lengths of each individual pair. The device returns a result with the following meaning:

- **normal**

  Indicates that the cable is operating properly
- **open**

  Indicates an interruption in the cable
- **short**

  Indicates a short circuit in the cable or the port is inactive
- **undefined**

  Indicates an untested cable or an unplugged cable

Network Monitoring with sFlow

SFlow is a standard protocol for monitoring networks. The device provides this function for visibility into network activity, enabling effective management and control of network resources.

The SFlow monitoring system consists of an SFlow agent, embedded in the device and a central SFlow collector. The agent uses sampling technology to capture the data packet statistics. SFlow instances associated with individual data sources within the agent perform packet flow and counter sampling. Using SFlow datagrams the agent forwards the sampled data packet statistics to an SFlow collector for analysis.

The agent uses 2 forms of sampling, a statistical packet based sampling of packet flows and a timed based sampling of counters. An SFlow datagram contains both types of samples. Packet flow sampling, based on a sampling rate, sends a steady, but random stream of datagrams to the collector. For time-based sampling, the agent polls the counters at set intervals to fill the datagrams.

The device implements datagram version 5 for the SFlow agent.

The user-defined SFlow functions are:

- Sampler configuration, packet flow sampling:
  - data source port number, to sample physical ports
  - receiver index associated with the sampler
  - Sampling rate

    The device counts the packets of received data. When the count reaches the user-defined number, the agent samples the packet.

    Range: **256..65535**

    0 = function inactive
  - Header size in bytes to sample

    Range: **20..256**
- Poller configuration, counter sampling:
  - data source port number, available for physical ports
  - receiver index associated with the poller
  - Interval, in seconds, between samples

    Range: **0..86400 (1 d)**
- Receiver configuration, up to 8 entries:
  - Owner name, to claim an SFlow entry
  - timeout, in seconds, until sampling is stopped and the device releases the receiver along with the sampler and the poller
  - datagram size
  - IP address
  - port number

To set up the SFlow agent for a monitoring session, first set up an available receiver, then, set up a sampling rate to perform packet flow sampling. Additionally, set up a polling interval for counter sampling.

For example, Company XYZ wishes to monitor data flow on a device. The IP address for the remote server containing the sFlow collector, is **10.10.10.10**. XYZ requires a sample of the first 256 bytes of every 300th packet. Furthermore, XYZ requires counter polling every 400 s.

Perform the following steps:

Step	Action
1	Navigate to **Diagnostics > SFlow > Receiver**.
2	For the name of the person or organization controlling the receiver, enter the value **XYZ** in the **Name** column.
3	For the remote server IP address, on which the SFlow collector software runs, specify the value **10.10.10.10** in the IP address column.
4	Navigate to the **Diagnostics > SFlow > Configuration**, **Sampler** tab.
5	In the Receiver column, select the index number of the receiver specified in the previous steps.
6	In the Sampling rate column, specify the value **300**.
7	In the Max. header size [byte] column, specify the value **256**.
8	Navigate to the **Diagnostics > SFlow > Configuration**, **Poller** tab.
9	In the Receiver column, select the index number of the receiver specified in the previous steps.

10	In the Interval [s] column, specify the value **400**.
11	To apply the settings, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sflow receiver 1 owner XYZ ip 10.10.10.10`	To set up an SFlow receiver
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`sflow sampler receiver 1 rate 300`	To assign the SFlow sampler on the port to the previously specified receiver with a sampling rate of **300**.
`sflow sampler maxheadersize 256`	To set up the maximum header size of the SFlow sampler to the value **256**.
`sflow poller receiver 1interval 400`	To assign the SFlow poller to the previously specified receiver and to sample data for **400** s.

Advanced Functions of the Device

DHCP Server

The Dynamic Host Configuration Protocol (DHCP) allows a server to assign the IP settings to the devices on the network (clients). This reduces the effort required for manual setup. The DHCP server stores and assigns the available IP addresses and further settings, if specified.

The procedure for assigning the IP settings consists of 4 phases:

- *DISCOVER* sent by the DHCP client
- *OFFER* sent by the DHCP server
- *REQUEST* sent by the DHCP client
- *ACKNOWLEDGE* sent by the DHCP server

The DHCP server in the device listens for requests on UDP port 67 and responds to the client devices on UDP port 68. When the device receives a DHCP request, it validates the IP address to be assigned before leasing the IP address and other IP settings to the requesting client device.

The device allows the activation of the DHCP Server function globally or on single physical ports.

Settings that the Server Assigns to the Clients

When operating as a DHCP server, the device assigns the IP settings to the client devices based on the following parameters:

- MAC address of the client device
- Physical port to which the client device is connected
- VLAN of which the client device is a member

The device assigns the following IP settings to the client devices:

- IP address
- Subnet mask
- Default gateway, if specified
- Further network settings, if specified

Pools

The device stores the IP settings in two types of pools.

- Static pools

  To assign the same IP address to a specific device each time, the device stores the relevant IP settings in a pool whose address range is exactly one IP address.

  Static pools are useful, for example, to assign a fixed IP address to a server, NAS, or printer.
- Dynamic pools

  To assign IP addresses from a certain address range, the device stores the relevant IP settings in a pool whose address range includes multiple IP addresses.

  Dynamic pools are useful, for example, to assign a certain IP address to client devices that belong to a certain VLAN.

Setting Up a Static Pool

In the following example, you set up the device to assign IP settings from a certain static pool to a certain client device connected to a certain port.

The static pool is to be set up based on the following parameters:

- MAC address of the client device: **ec:e5:55:d6:50:01**
- Physical port to which the client device is connected on the server device: **1/1**
- IP address that the device should assign to the client device: **192.168.23.42**
- The assigned IP settings are valid for 2 days: **172800**

Perform the following steps:

Step	Action
1	Navigate to **Advanced > DHCP > DHCP Server > Pool**.
2	Add a table row. To do this, click the ⊞ button.
3	• Specify the following settings for the table row: ◦ IP range start column = **192.168.23.42** ◦ Port column = **1/1** ◦ MAC address column = **ec:e5:55:d6:50:01** ◦ Lease time [s] column = **172800** ◦ Active column = selected
4	To apply the settings, click the ✓ button.
5	Navigate to **Advanced > DHCP > DHCP Server > Global**.
6	Verify that the DHCP function is active on port **1/1**. If not already done, select the checkbox in the DHCP server active column for port **1/1**.
7	Enable the DHCP server globally. Select the **On** radio button in the Operation frame.
8	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dhcp-server pool add 1 static 192.168.23.42`	To add a static pool with index **1** with the IP address **192.168.23.42**.
`dhcp-server pool modify 1 mode interface 1/1`	To assign the static pool with index **1** to physical port **1/1**.
`dhcp-server pool modify 1 mode mac EC:E5:55:D6:50:01`	To assign the static pool with index **1** to a client device with MAC address **EC:E5:55:D6:50:01**.
`dhcp-server pool modify 1 leasetime 172800`	To specify the lease time of the static pool with index **1**.
`dhcp-server pool mode 1 enable`	To enable the static pool with index **1**.
`dhcp-server operation`	To enable the DHCP server globally.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`dhcp-server operation`	To activate the DHCP server function on this port.

Setting Up a Dynamic Pool

In the following example, you set up the device to assign an IP address from a certain address range to client devices connected to a certain port.

The dynamic pool is to be set up based on the following parameters:

- MAC address of the client device or further information in the DHCP request is not to be evaluated.
- Physical port to which the client devices are connected on the server device: **1/2**
- Address range from which the device assigns an IP address to the client devices: **192.168.23.92..192.168.23.142**
- The assigned IP settings are valid for 2 days: **172800**

Perform the following steps:

Step	Action
1	Navigate to **Advanced > DHCP > DHCP Server > Pool**.
2	Add a table row. To do this, click the ⊞ button.
3	Specify the following settings for the table row: • IP range start column = **192.168.23.92** • IP range end column = **192.168.23.142** • Port column = **1/2** • Lease time [s] column = **172800** • Active column = **Selected**
4	To apply the settings, click the ✓ button.
5	Navigate to **Advanced > DHCP > DHCP Server > Global**.
6	Verify that the DHCP function is active on port **1/2**. If not already done, select the checkbox in the DHCP server active column for port **1/2**.
7	Enable the DHCP server globally. Select the **On** radio button in the Operation frame.
8	To apply the settings, click the ✓ button.

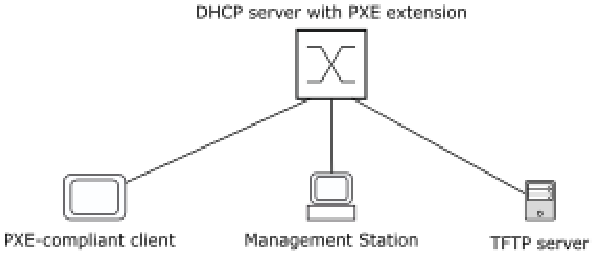
Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dhcp-server pool add 2 dynamic 192.168.23.92 192.168.23.142`	To add a dynamic pool with index **2** with a range from **192.168.23.92** to **192.168.23.142**.
`dhcp-server pool modify 2 mode interface 1/2`	To assign the static pool with index **2** to physical port **1/2**.
`dhcp-server pool modify 2 leasetime 172800`	To specify the lease time of the dynamic pool with index **2**.
`dhcp-server pool mode 2 enable`	To enable the dynamic pool with index **2**.
`dhcp-server operation`	To enable the DHCP server globally.
`interface 1/2`	To change to the Interface Configuration mode of interface **1/2**.
`dhcp-server operation`	To activate the DHCP server function on this port.

Setting Up a Preboot eXecution Environment (PXE)

The device allows boot parameters for PXE-compliant clients to boot a bootloader image downloaded from a TFTP server. Possible applications include booting an installation environment, a rescue system, or a live system over the network. A typical use case is an infotainment device that boots an operating system supplied over the network.

Structure of a Preboot eXecution Environment (PXE) setup



To activate the PXE boot extension for a specific pool, you add the following values to the pool settings:

- *Vendor Identifier*
- *Client System Architecture*
- URL to a bootloader image file on a TFTP server

The device expects the information for *Vendor Identifier* and *Client System Architecture* in summarized form as the *Class Identifier* in the **DHCP option 60** field. When a PXE-compliant client device broadcasts a *DHCP Discover* message with a matching *Class Identifier* in the **DHCP option 60** field, the device responds with the settings specified in the relevant pool.

A PXE-compliant client device requires a bootloader image that matches its hardware architecture. When planning, keep in mind that you need at least one pool for each required hardware architecture.

> **NOTE:** The device does not verify the integrity, authenticity and availability of the TFTP servers and the bootloader image files involved. Use the PXE boot extension only if you trust the transfer network.

In the following example, the network administrator wants you to specify the PXE boot extension parameters for an existing DHCP Server Pool item.

Class Identifier in the **DHCP option 60** field	*Vendor Identifier*	**vendor1**
	Client System Architecture	**efi-x86-64**
Bootloader image file on the TFTP server		**tftp://192.168.1.5/boot-efi-x86-64.img**

When modifying an existing DHCP Server Pool item, you need to deactivate the pool first. For information on how to set up a DHCP server pool, refer to Setting Up a Static Pool, page 324 or Setting Up a Dynamic Pool, page 325. After modifying the DHCP Server Pool item, you reactivate the pool.

Perform the following steps:

Step	Action
1	Navigate to **Advanced** **>** **DHCP** **>** **DHCP Server** **>** **Pool**.
2	Deactivate the DHCP Server Pool item. To do this, clear the checkbox in the Active column.
3	To apply the settings, click the ✓ button.
4	In the Vendor ID column, enter the string **vendor1**.
5	In the Client Architecture column, select the **efi-x86-64** item from the drop-down list.
6	In the Configuration URL column, enter the URL: **tftp://192.168.1.5:/boot-efi-x86-64.img**.
7	Reactivate the DHCP Server Pool item. To do this, select the checkbox in the Active column.
8	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dhcp-server pool mode 1 disable`	To deactivate pool **1**.
`dhcp-server pool modify 1 mode classid vendorid vendor1`	To enable the PXE boot extension for pool **1** and assign the string **vendor1** as the *Vendor Identifier*.
`dhcp-server pool modify 1 mode classid architecture efi-x86-64`	To specify the value **efi-x86-64** as the *Client System Architecture*.
`dhcp-server pool modify 1 option configpath tftp://192.168.1.5:/boot-efi-x86-64.img`	To specify the URL **tftp://192.168.1.5/boot-efi-x86-64.img** to the bootloader image file on a TFTP server.
`dhcp-server pool mode 1 enable`	To reactivate pool **1**.
`show dhcp-server pool 1`	To display the settings specified for pool **1**.

```
DHCP Server Pool
----------------
Index...........................1
...
PXE Client Vendor ID...........vendor1
PXE Client Architecture........efi-x86-64
Configuration URL............. tftp://192.168.1.5:/boot-efi-x86-64.img
...
```

DHCP L2 Relay

On the front panel of the device you find the following hazard message:

⚠WARNING

UNINTENDED OPERATION

Do not change cable positions if DHCP Option 82 is enabled. Verify the user guide before servicing.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

A network administrator uses the DHCP Layer 2 *Relay Agent* to add DHCP client information. This information is required by Layer 3 *Relay Agents* and DHCP servers to assign an address and configuration to a client.

When a DHCP client and server are in the same IP subnet, they exchange IP address requests and replies directly. However, having a DHCP server on each subnet is expensive and often impractical. An alternative to having a DHCP server in every subnet is to use the network devices to relay packets between a DHCP client and a DHCP server located in a different subnet.

A Layer 3 *Relay Agent* is generally a router that has IP interfaces in both the client and server subnets and routes the data packets between them. However, in Layer 2 switched networks, there are one or more network devices, switches for example, between the client and the Layer 3 *Relay Agent* or DHCP server. In this case, this device provides a Layer 2 *Relay Agent* to add the information that the Layer 3 *Relay Agent* and DHCP server require to perform their roles in address and configuration assignment.

For the DHCPv6 protocol, a *Relay Agent* is used to add *Relay Agent* options to DHCPv6 packets exchanged between a client and a DHCPv6 server. The Lightweight DHCPv6 Relay Agent (LDRA) is described in RFC 6221.

The LDRA processes 2 types of messages:

- The first type of message is the *Relay-Forward* message which contains unique information about the client.
- The second type of message is the *Relay-Reply* message which the DHCPv6 server sends to the *Relay Agent*. The *Relay Agent* then validates the message to include the information encapsulated in the initial *Relay-Forward* message and if valid, sends the packet to the client.

The *Relay-Forward* message contains *Interface-ID* information, defined as *Option 18*. This option provides information that identifies the interface on which the client request was sent. The device discards DHCPv6 packets that do not contain *Option 18* information.

Circuit and Remote IDs

In an IPv4 environment, before forwarding the request of a client to the DHCP server, the device adds the *Circuit ID* and the *Remote ID* to the **Option 82** field of the DHCP request packet.

- The *Circuit ID* stores on which port the device received the request of the client.
- The *Remote ID* contains the MAC address, the IP address, the system name, or a user-defined character string. Using it, the participating devices identify the *Relay Agent* that received the request of the client.

The device and other *Relay Agents* use this information to re-direct the answer from the DHCP *Relay Agent* to the original client. The DHCP server can analyze this data for example to assign the client an IP address from a specific address pool.

Also, the replay packet of the DHCP server contains the *Circuit ID* and the *Remote ID*. Before forwarding the answer to the client, the device removes the information from the **Option 82** field.

DHCP L2 Relay Configuration

The **Advanced > DHCP L2 Relay > Configuration** dialog allows the activation of the function on the active ports and on the VLANs. In the Operation frame, select the **On** radio button, then click the ✓ button.

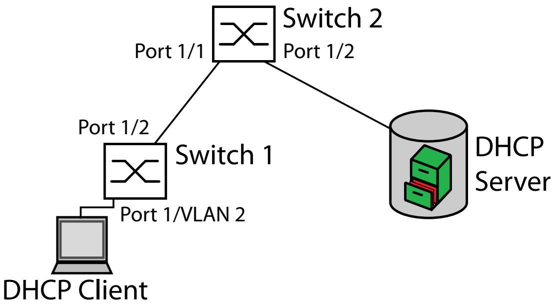
The device forwards DHCPv4 packets with *Option 82* information and DHCPv6 packets with *Option 18* information on those ports for which the checkbox in the

Active column and in the Trusted port column is selected. Typically, these are ports in the network of the DHCP server.

The ports to which the DHCP clients are connected, you activate the DHCP L2 Relay function, but leave the Trusted port checkbox cleared. On these ports, the device discards DHCPv4 packets with *Option 82* information and DHCPv6 packets with *Option 18* information.

An example configuration for the DHCPv4 L2 Relay function is shown below. The configuration steps for DHCPv6 L2 Relay function are similar, except for the *Circuit ID* and *Remote ID* entries that can only be specified for *Option 82*.

DHCP Layer 2 Example Network:



Perform the following steps on Switch 1:

Step	Action
1	Navigate to the **Advanced > DHCP L2 Relay > Configuration**, **Interface** tab.
2	For port **1/1**, specify the settings as follows: • Select the checkbox in the Active column.
3	For port **1/2**, specify the settings as follows: • Select the checkbox in the Active column. • Select the checkbox in the Trusted port column.
4	Navigate to the **Advanced > DHCP L2 Relay > Configuration**, **VLAN ID** tab.
5	Specify the settings for VLAN 2 as follows: • Select the checkbox in the Active column. • Select the checkbox in the Circuit ID column. • To use the IP address of the device as the *Remote ID*, in the Remote ID type column, specify the value **ip**.
6	Enable the DHCP L2 Relay function. Select the **On** radio button in the Operation frame.
7	To apply the settings, click the ✓ button.

Perform the following steps on Switch 2:

Step	Action
1	Navigate to the **Advanced > DHCP L2 Relay > Configuration**, **Interface** tab.
2	For port **1/1** and **1/2**, specify the settings as follows: • Select the checkbox in the Active column. • Select the checkbox in the Trusted port column.
3	Enable the DHCP L2 Relay function. Select the **On** radio button in the Operation frame.
4	To apply the settings, click the ✓ button.

Verify that VLAN 2 is present, then perform the following step on Switch 1:

- Set up VLAN 2, and specify port **1/1** as a member of VLAN 2.

Execute the following commands:

Command	**Description**
`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`dhcp-l2relay circuit-id 2`	To activate the Circuit ID and the DHCP Option 82 on VLAN **2**.
`dhcp-l2relay remote-id ip 2`	To specify the IP address of the device as the Remote ID on VLAN **2**.
`dhcp-l2relay mode 2`	To activate the DHCP L2 Relay function on VLAN **2**.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`dhcp-l2relay mode`	To activate the DHCP L2 Relay function on the port.
`exit`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface **1/2**.
`dhcp-l2relay trust`	To specify the port as Trusted port.
`dhcp-l2relay mode`	To activate the DHCP L2 Relay function on the port.
`exit`	To change to the Configuration mode.
`dhcp-l2relay mode`	To enable the DHCP L2 Relay function in the device.

Perform the following steps on Switch 2:

Command	**Description**
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`dhcp-l2relay trust`	To specify the port as Trusted port.
`dhcp-l2relay mode`	To activate the DHCP L2 Relay function on the port.
`exit`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface **1/2**.
`dhcp-l2relay trust`	To specify the port as Trusted port.
`dhcp-l2relay mode`	To activate the DHCP L2 Relay function on the port.
`exit`	To change to the Configuration mode.
`dhcp-l2relay mode`	To enable the DHCP L2 Relay function in the device.

Using the Device as a DNS Client

As a DNS client, the device queries a DNS server to resolve the hostname of a device in the network to the related IP address.

The device allows up to four DNS servers to which it forwards a request to resolve a hostname (*DNS request*).

As an alternative, the device can obtain the DNS server addresses from a DHCP server. For this, the DHCP server needs to be reachable in the same VLAN as the management of the device.

The device allows the hostname and IP address of defined devices in the network to be manually entered into the device. You can enter up to 64 static hosts.

When the device receives a request to resolve a hostname (*DNS request*), it first tries to find the related IP address internally. If the device cannot resolve the hostname by itself, it forwards the request to a DNS server. The DNS server returns the associated IP address to the device.

Optionally, the device caches this response for future queries. The device caches up to 128 DNS server responses consisting of hostname and related IP address.

Setting Up the *DNS Client* Function

The device has the option to contact a DNS server assigned by the DHCP server. This example describes how to set up the device to contact a user-defined DNS server instead. To do this, perform the following steps:

Step	Action
1	Navigate to **Advanced > DNS > Client > Static**.
2	In the Configuration frame, select the **user** item from the Source drop-down list.
3	In the Configuration frame, **Domain name** field, specify the value **example.com**.
4	In the table, click the ⊞ button. The dialog displays the Create window.
5	In the Index column, specify the value **1** as the sequential number. You can only assign unique values.
6	In the IP address column, specify the IPv4 address of the DNS server, for example **192.168.3.5**. You can also specify a valid IPv6 address.
7	Click **OK**. The device adds a table row.
8	Navigate to **Advanced > DNS > Client > Global**.
9	Enable the Client function. Select the **On** radio button in the Operation frame.
10	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dns client source user`	To specify that the device contacts a user-defined DNS server.
`dns client domain-name example.com`	To specify the string **example.com** as a domain name. The device adds this domain name to hostnames without a domain suffix.
`dns client servers add 1 ip 192.168.3.5`	To add a DNS server with the IPv4 address **192.168.3.5** as index **1**.
`dns client servers add 2 ip 2001::1`	To add a DNS server with the IPv6 address **2001::1** as index **2**.
`dns client adminstate`	To enable the Client function globally.

Setting Up a Static Host

This example shows how to manually map an IP address to a hostname. To do this, perform the following steps:

Step	Action
1	Navigate to **Advanced** > **DNS** > **Client** > **Static Hosts**.
2	In the table, click the ⊞ button. The dialog displays the Create window.
3	In the Index column, specify the value **1**.
4	In the **Name** column, enter the hostname, for example **device1**.
5	In the IP address column, specify the IPv4 address to be mapped to the hostname, for example **192.168.3.9**. You can also specify a valid IPv6 address.
6	Click **OK**. The device adds a table row. The device sends data packets directed to **device1** to the recipient with the IP address **192.168.3.9**.
7	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dns client host add 1 name device1 ip 192.168.3.9`	To map the hostname **device1** with the IP address **192.168.3.9**.
`dns client adminstate`	To enable the Client function globally.

GARP Function

The Generic Attribute Registration Protocol (GARP) is defined by the IEEE standards association to provide a generic framework so switches can register and deregister attribute values, such as VLAN identifiers and multicast group membership.

If an attribute for a participant is registered or deregistered according to the GARP function, the participant is modified according to specific rules. The participants are a set of reachable end stations and network devices. The defined set of participants at any given time, along with their attributes, is the reachability tree for the subset of the network topology. The device forwards the data frames only to the registered end stations. The station registration helps prevent attempts to send data to the end stations that are unreachable.

Configuring GMRP

The GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) that provides a mechanism allowing network devices and end stations to dynamically register group membership. The devices register group membership information with the devices attached to the same LAN segment. The GARP function also allows the devices of disseminate the information across the network devices that support extended filtering services.

NOTE: Before you enable the GMRP function, verify that the MMRP function is disabled.

The following example describes the configuration of the GMRP function. The device provides a constrained multicast flooding facility on a selected port.

Perform the following steps:

Step	Action
1	Navigate to **Switching > GARP > GMRP**.
2	To provide constrained *Multicast Flooding* on a port, select the checkbox in the GMRP active column.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`garp gmrp operation`	To enable the GMRP function on the port.
`exit`	To change to the Configuration mode.
`garp gmrp operation`	To enable the GMRP function globally.

Configuring GVRP

You use the GVRP function to allow the device to exchange VLAN configuration information with other GVRP-capable devices. Thus reducing unnecessary traffic of broadcast and undefined unicast data packets. Besides, the GVRP function dynamically sets up VLANs on devices connected through 802.1Q trunk ports.

The following example describes the configuration of the GVRP function. The device allows exchange of VLAN configuration information with other GVRP-capable devices.

Perform the following steps:

Step	Action
1	Navigate to **Switching > GARP > GVRP**.
2	To exchange VLAN configuration information with other GVRP-capable devices, select checkbox in the GVRP active column for the port.
3	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 3/1`	To change to the Interface Configuration mode of interface **3/1**.
`garp gvrp operation`	To enable the GVRP function on the port.
`exit`	To change to the Configuration mode.
`garp gvrp operation`	To enable the GVRP function globally.

MRP-IEEE

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP-IEEE) to replace the Generic Attribute Registration Protocol (GARP). The IEEE standards association also modified and replaced the GARP applications, GARP Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP), with the Multiple MAC Registration Protocol (MMRP) and the Multiple VLAN Registration Protocol (MVRP).

To confine forwarding the data packets to the required areas of a network, the MRP-IEEE applications distribute attribute values to MRP-IEEE enabled devices across a LAN. The MRP-IEEE applications register and de-register multicast group memberships and VLAN identifiers.

> **NOTE:** The Multiple Registration Protocol (MRP-IEEE) requires a loop free network. To help prevent loops in the network, use a network protocol such as the Media Redundancy Protocol (MRP), Spanning Tree Protocol (STP), or Rapid Spanning Tree Protocol (RSTP) with MRP-IEEE.

MRP-IEEE Operation

Each participant contains an applicant component and an MRP Attribute Declaration (MAD) component. The applicant component forms the attribute values and their registration and de-registration. The MAD component generates MRP-IEEE messages for transmission and processes messages received from other participants. The MAD component encodes and transmits the attributes to other participants in MRP Data Units (MRPDU). In the switch, an MRP Attribute Propagation (MAP) component distributes the attributes to participating ports.

A participant exists for each MRP-IEEE application and each LAN port. For example, a participant application exists on an end device and another application exists on a switch port. The Applicant state machine records the attribute and port for each MRP participant declaration on an end device or switch. Applicant state machine variable changes trigger the transmission of MRPDUs to communicate the declaration or withdrawal.

To establish an MMRP instance, an end device first sends a Join empty (JoinMt) message with the appropriate attributes. The switch then floods the JoinMt to the participating ports and to the neighboring switches. The neighboring switches flood the message to their participating port, and so on, establishing a path for the group data packets.

MRP-IEEE Timers

The default timer settings help prevent unnecessary attribute declarations and withdrawals. The timer settings allow the participants to receive and process MRP-IEEE messages before the *Leave* or *LeaveAll* timers expire.

When you reconfigure the timers, maintain the following relationships:

- To allow for re-registration after a *Leave* or *LeaveAll* event, even if there is a lost message, specify the *Leave* timer value ≥ `(2x JoinTime) + 60 in 1/100 s`.
- To minimize the volume of *Rejoin* data packets the device generates following a *LeaveAll* event, specify the value for the *LeaveAll* timer larger than the *Leave* timer value.

The following list contains various MRP-IEEE events that the device transmits:

- *Join*

  Controls the interval for the next *Join* message transmission.
- *Leave*

  Controls the length of time that a switch waits in the *Leave* state before changing to the withdrawal state.
- *LeaveAll*

  Controls the frequency with which the switch generates *LeaveAll* messages.

When expired, the Periodic timer initiates a Join request MRP-IEEE message that the switch sends to participants on the LAN. The switches use this message to help prevent unnecessary withdrawals.

MMRP

When a device receives broadcast, multicast or undefined data packets on a port, the device floods the data packets to the other ports. This process causes unnecessary use of bandwidth on the LAN.

The Multiple MAC Registration Protocol (MMRP) allows control of data packets flooding by distributing an attribute declaration to participants on a LAN. The attribute values that the MAD component encodes and transmits on the LAN in MRP-IEEE messages are Group service requirement information and 48-bit MAC addresses.

The switch stores the attributes in a filtering database as MAC address registration entries. The forwarding process uses the filtering database entries only to transmit data through those ports necessary to reach Group member LANs.

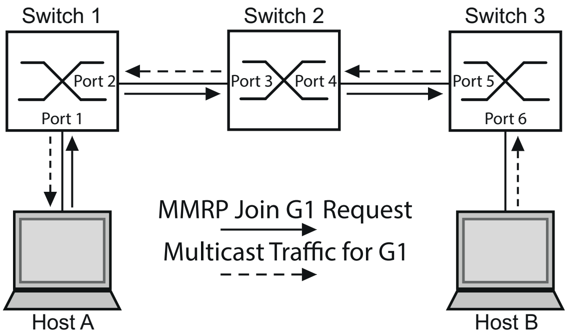
Switches facilitate the group distribution mechanisms based on the Open Host Group concept, receiving packets on the active ports and forwarding only to ports with group members. This way, any MMRP participants requiring packets transmitted to a particular group or groups, requests membership in the group. MAC service users send packets to a particular group from anywhere on the LAN. A group receives these packets on the LANs attached to registered MMRP participants. MMRP and the MAC Address Registration Entries thus restrict the packets to required segments of a loop-free LAN.

To maintain the registration and deregistration state and to receive data packets, a port declares interest periodically. Every device on a LAN with the MMRP function enabled maintains a filtering database and forwards the data packets with the group MAC addresses to the listed participants.

Setting Up MMRP

In this example, Host A intends to listen to the data packets destined for group G1. Switch A processes the MMRP Join request received from host A and sends the request to both of the neighboring switches. The devices on the LAN now recognize that there is a host that receives the data packets destined for group G1. When Host B starts transmitting data destined for group G1, the data flows on the path of registrations and Host A receives it.

MMRP Network for MAC address Registration:



Enable the MMRP function on the switches. To do this, perform the following steps:

Step	Action
1	Navigate to the **Switching > MRP-IEEE > MMRP**, **Configuration** tab.
2	To activate port **1** and port **2** as MMRP participants, select the checkbox in the MMRP column for port **1** and port **2** on switch 1.
3	To activate port **3** and port **4** as MMRP participants, select the checkbox in the MMRP column for port **3** and port **4** on switch 2.
4	To activate port **5** and port **6** as MMRP participants, select the checkbox in the MMRP column for port **5** and port **6** on switch 3.
5	To send periodic events allowing the device to maintain the registration of the MAC address group, enable the Periodic state machine. Select the **On** radio button in the Configuration frame.
6	To apply the settings, click the ✓ button.

To enable the MMRP ports on switch 1, use the following commands. Substituting the appropriate interfaces in the commands, enable the MMRP functions and ports on switches 2 and 3.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`mrp-ieee mmrp operation`	To enable the MMRP function on the port.
`interface 1/2`	To change to the Interface Configuration mode of interface **1/2**.
`mrp-ieee mmrp operation`	To enable the MMRP function on the port.
`exit`	To change to the Configuration mode.
`mrp-ieee mrp periodic-state-machine`	To enable the Periodic state machine function globally.
`mrp-ieee mmrp operation`	To enable the MMRP function globally.

MVRP

The Multiple VLAN Registration Protocol (MVRP) is an MRP-IEEE application that provides dynamic VLAN registration and withdrawal services on a LAN.

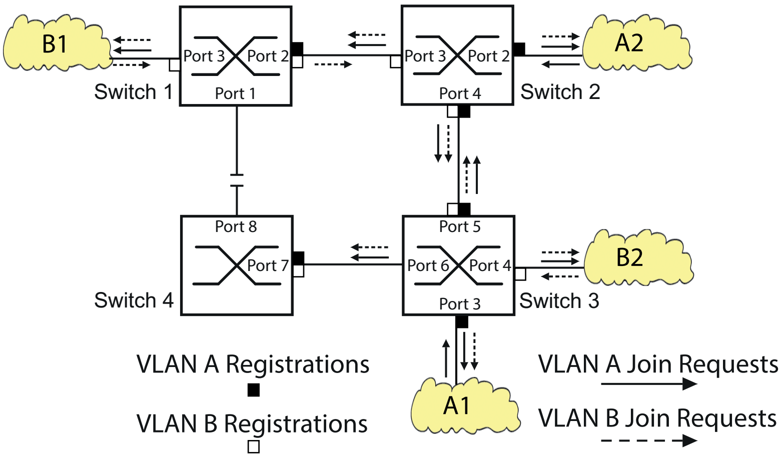
The MVRP function provides a maintenance mechanism for the Dynamic VLAN Registration Entries, and for transmitting the information to other devices. This information allows MVRP-aware devices to establish and update their VLAN membership information. When members are present on a VLAN, the information indicates through which ports the switch forwards the data packets to reach those members.

The main purpose of the MVRP function is to allow switches to discover some of the VLAN information that you otherwise manually set up. Discovering this information allows switches to overcome the limitations of bandwidth consumption and convergence time in large VLAN networks.

MVRP Example

Set up a network comprised of MVRP aware switches (1-4) connected in a ring topology with end device groups, A1, A2, B1, and B2 in 2 different VLANs, A and B. With STP enabled on the switches, the ports connecting switch 1 to switch 4 are in the *discarding* state, helping prevent a loop condition.

MVRP Example Network for VLAN Registration:



In the MVRP example network, the LANs first send a Join request to the switches. The switch enters the VLAN registration in the MAC address table (forwarding database) for the port receiving the frames.

The switch then propagates the request to the other ports, and sends the request to the neighboring LANs and switches. This process continues until the switches have registered the VLANs in the MAC address table (forwarding database) of the receive port.

Enable MVRP on the switches. To do this, perform the following steps:

Step	Action
1	Navigate to the **Switching** > **MRP-IEEE** > **MVRP**, **Configuration** tab.
2	To activate the ports **1** through **3** as MVRP participants, select the checkbox in the MVRP column for the ports **1** through **3** on switch 1.
3	To activate the ports **2** through **4** as MVRP participants, select the checkbox in the MVRP column for the ports **2** through **4** on switch 2.
4	To activate the ports **3** through **6** as MVRP participants, select the checkbox in the MVRP column for the ports **3** through **6** on switch 3.
5	To activate port **7** and port **8** as MVRP participants, select the checkbox in the MVRP column for port **7** and port **8** on switch 4.
6	To maintain the registration of the VLANs, enable the Periodic state machine. Select the **On** radio button in the Configuration frame.
7	Enable the MVRP function. Select the **On** radio button in the Operation frame.
8	To apply the settings, click the ✓ button.

To enable the MVRP ports on switch 1, use the following commands. Substituting the appropriate interfaces in the commands, enable the MVRP functions and ports on switches 2, 3 and 4.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`mrp-ieee mvrp operation`	To enable the MVRP function on the port.
`interface 1/2`	To change to the Interface Configuration mode of interface **1/2**.
`mrp-ieee mvrp operation`	To enable the MVRP function on the port.
`exit`	To change to the Configuration mode.
`mrp-ieee mvrp periodic-state-machine`	To enable the Periodic state machine function globally.
`mrp-ieee mvrp operation`	To enable the MVRP function globally.

Industry Protocols

IEC 61850/MMS

IEC 61850/MMS is an industrial communication protocol standardized by the International Electrotechnical Commission (IEC). The protocol is to be found in substation automation, for example in the control technology of energy suppliers.

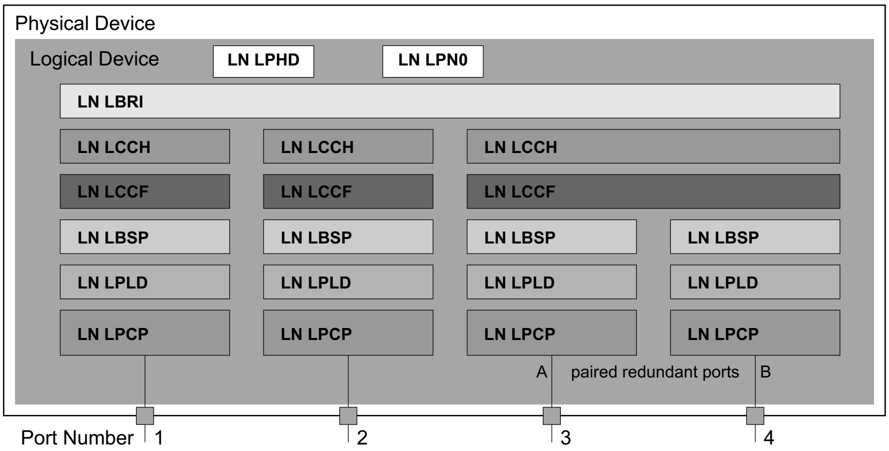
This protocol, which works in a packet-oriented way, is based on the TCP/IP transport protocol and uses the Manufacturing Messaging Specification (MMS) for the client-server communication. The protocol is object-oriented and defines a standardized configuration language that comprises, among other things, functions for SCADA, Intelligent Electronic Devices (IED) and for the network control technology.

Part 6 of the IEC 61850 standard defines the configuration language SCL (Substation Configuration Language). SCL describes the properties of the device and the system structure in an automatically processable form. The properties of the device described with SCL are stored in the ICD file in the device.

Switch Model for IEC 61850

The Technical Report, IEC 61850 90-4, specifies a bridge model. The bridge model represents the functions of a switch as objects of an Intelligent Electronic Device (IED). An MMS client (for example the control room software) uses these objects to monitor and set up the device.

Bridge model based on Technical Report IEC 61850 90-4:



Classes of the bridge model based on TR IEC61850 90-4:

Class	Description
`LN LLN0`	**Zero** logical node of the **Bridge** IED: Defines the logical properties of the device.
`LN LPHD`	**Physical Device** logical node of the **Bridge** IED: Defines the physical properties of the device.
`LN LBRI`	**Bridge** logical node: Represents general settings of the bridge functions of the device.
`LN LCCH`	**Communication Channel** logical node: Defines the logical **Communication Channel** that consists of one or more physical ports.
`LN LCCF`	**Channel Communication Filtering** logical node: Defines the VLAN and multicast settings for the greater-level **Communication Channel**.
`LN LBSP`	**Port Spanning Tree Protocol** logical node: Defines the Spanning Tree statuses and settings for the respective physical port.
`LN LPLD`	**Port Layer Discovery** logical node: Defines the LLDP statuses and settings for the respective physical port.
`LN LPCP`	**Physical Communication Port** logical node: Represents the respective physical port.

Integration Into a Control System

Preparation of the Device

Perform the following steps:

- Verify that the device has an IP address assigned.
- Navigate to **Advanced > Industrial Protocols > IEC 61850-MMS**.
- Start the MMS server.

  Select the **On** radio button in the Operation frame and click the ✓ button.

  Afterwards, an MMS client can connect to the device and to read and monitor the objects defined in the bridge model.

IEC 61850/MMS does not provide any authentication mechanisms. If the write access for IEC 61850/MMS is activated, every client that can access the device using TCP/IP is capable of changing the settings of the device. As a result, incorrect device settings and potential network interruptions may occur.

NOTICE

UNAUTHORIZED ACCESS

Only activate the write access if you have taken additional measures (for example Firewall, VPN, etc.) to reduce possible unauthorized access.

Failure to follow these instructions can result in equipment damage.

To allow the MMS client to change the settings, select the Write access checkbox, and click the ✓ button.

Offline Configuration

The device allows the ICD file to be downloaded using the Graphical User Interface. This file contains the properties of the device described with SCL and allows the substation to be set up without directly connecting to the device.

- Navigate to **Advanced > Industrial Protocols > IEC 61850-MMS**.
- To load the ICD file to your PC, click the ⤓ button.

Monitoring the Device

The IEC 61850/MMS server integrated into the device allows multiple statuses of the device to be monitored by means of the Report Control Block (RCB). Up to 5 MMS clients can register for a Report Control Block at the same time.

The device allows the following statuses to be monitored with IEC 61850/MMS:

Class	RCB object	Description
`LN LPHD`	`TmpAlm`	When the temperature measured in the device exceeds or falls below the specified temperature threshold values, the status changes.
	`PhyHealth`	When the status of the **LPHD.TmpAlm** RCB object changes, the status changes.
`LN LPHD`	`TmpAlm`	When the temperature measured in the device exceeds or falls below the specified temperature threshold values, the status changes.
	`PwrSupAlm`	When one of the redundant power supplies becomes inoperable or starts operating again, the status changes.
	`PhyHealth`	When the status of the **LPHD.PwrSupAlm** or **LPHD.TmpAlm** RCB object changes, the status changes.
`LN LBRI`	`RstpRoot`	When the device takes over or relinquishes the role of the *Root bridge*, the status changes.
	`RstpTopoCnt`	When the topology changes due to a change of the *Root bridge*, the status changes.
`LN LCCH`	`ChLiv`	When the link status of the physical port changes, the status changes.
`LN LPCP`	`PhyHealth`	When the link status of the physical port changes, the status changes.

Modbus TCP Function

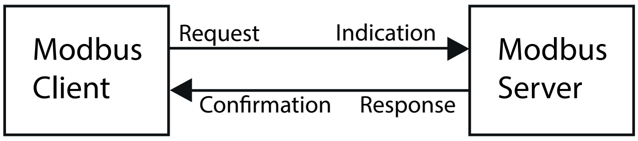
Modbus TCP is an application layer messaging protocol providing client/server communication between the client and devices connected in Ethernet TCP/IP networks.

The Modbus TCP function allows the device to be installed in networks already using Modbus TCP and retrieve information saved in the registers in the device.

Client/Server Modbus TCP/IP Mode

The device supports the client/server model of Modbus TCP/IP. This device operates as a server in this constellation and responds to requests from a client for information saved in the registers.

Client/Server Modbus TCP/IP Mode:



The client / server model uses four types of messages to exchange data between the client and server:

- Modbus TCP/IP Request, the client generates a request for information and sends it to the server.
- Modbus TCP/IP Indication, the server receives a request as an indication that a client requires information.
- Modbus TCP/IP Response, when the required information is available, the server sends a reply containing the requested information. When the requested information is unavailable, the server sends an Exception Response to notify the client of the error detected during the processing. The Exception Response contains an exception code indicating the reason for the detected error.
- Modbus TCP/IP Confirmation, the client receives a response from the server, containing the requested information.

Supported Functions and Memory Mapping

The device supports functions with the public codes **0x03** (**Read Holding Registers**) and **0x05** (**Write Single Coil**). The codes let you read the information saved in the registers such as the system information, including the system name, system location, software version, IP address, MAC address. The codes also let you read the port information and port statistics. The **0x05** code allows port counters to be reset individually or globally.

The following list contains definitions for the values entered in the **Format** column:

- Bitmap: a group of 32-bits, encoded into the Big-endian byte order and saved in 2 registers. Big-endian systems save the most significant byte of a word in the smallest address and save the least significant byte in the largest address.
- F1: 16-bit unsigned integer
- F2: Enumeration - power supply alarm
  - 0 = power supply good
  - 1 = power supply error detected
- F3: Enumeration - OFF/ON
  - 0 = Off
  - 1 = On
- F4: Enumeration - port type
  - 0 = Giga - Gigabit Interface Converter (GBIC)
  - 1 = Copper - Twisted-Pair (TP)
  - 2 = Fiber - 10 Mbit/s
  - 3 = Fiber - 100 Mbit/s
  - 4 = Giga - 10/100/1000 Mbit/s (triple speed)
  - 5 = Giga - Copper 1000 Mbit/s TP
  - 6 = Giga - Small Form-factor Pluggable (SFP)
- F9: 32-bit unsigned long
- String: octets, saved in sequence, 2 octets per register.

Modbus TCP/IP Codes

The addresses in the following tables allow the client to reset port counters and retrieve specific information from the device registers.

System/Global Information:

Address	Qty	Description	Min	Max	Step	Unit	Format
0000	128	System Name	-	-	-	-	String
0080	128	System Contact	-	-	-	-	String
0100	128	System Location	-	-	-	-	String
0180	128	Software Version	-	-	-	-	String
0200	32	OrderCode	-	-	-	-	String
0220	16	Serial Number	-	-	-	-	String
0230	1	IP Address[0]	0	254	1	-	F1
0231	1	IP Address[1]	0	254	1	-	F1
0232	1	IP Address[2]	0	254	1	-	F1
0233	1	IP Address[3]	0	254	1	-	F1
0234	1	NetMask[0]	0	255	1	-	F1
0235	1	NetMask[1]	0	255	1	-	F1
0236	1	NetMask[2]	0	255	1	-	F1
0237	1	NetMask[3]	0	255	1	-	F1
0238	1	GateWay[0]	0	254	1	-	F1
0239	1	GateWay[1]	0	254	1	-	F1
023A	1	GateWay[2]	0	254	1	-	F1
023B	1	GateWay[3]	0	254	1	-	F1
023C	3	MacAddress	-	-	-	-	String
023F	1	PowerAlarm1	0	1	1	-	F2
0240	1	PowerAlarm2	0	1	1	-	F2
0241	1	StpState	0	1	1	-	F1
0242	2	Number of Ports	1	64	1	-	F1
0244	1	Reset Counter (all Counter)	0	1	1	-	F1
0245	4	Port Present Map	-	-	-	-	Bitmap
0249	4	Port Link Map	-	-	-	-	Bitmap
024D	4	Port Stp State Map	-	-	-	-	Bitmap
0251	4	Port Activity Map	-	-	-	-	Bitmap

Port Information:

Address	Qty	Description	Min	Max	Step	Unit	Format
0400	1	Port 1 Type	0	6	1	-	F4
0401	1	Port 2 Type	0	6	1	-	F4
		...					
043F	1	Port 64 Type	0	6	1	-	F4
0440	1	Port 1 Link Status	0	1	1	-	F1
0441	1	Port 2 Link Status	0	1	1	-	F1
		...					
047F	1	Port 64 Link Status	0	1	1	-	F1
0480	1	Port 1 STP State	0	1	1	-	F1
0481	1	Port 2 STP State	0	1	1	-	F1
		...					
04BF	1	Port 64 STP State	0	1	1	-	F1
04C0	1	Port 1 Activity	0	1	1	-	F1
04C1	1	Port 2 Activity	0	1	1	-	F1
		...					
04FF	1	Port 64 Activity	0	1	1	-	F1
0500	1	Port 1 Counter Reset	0	1	1	-	F1
0501	1	Port 2 Counter Reset	0	1	1	-	F1
		...					
053F	1	Port 64 Counter Reset	0	1	1	-	F1

Port Statistics:

Address	Qty	Description	Min	Max	Step	Unit	Format
0800	2	Port1 - Number of bytes received	0	4294967295 $(2^{32}-1)$	1	-	F9
0802	2	Port1 - Number of bytes sent	0	4294967295	1	-	F9
0804	2	Port1 - Number of frames received	0	4294967295	1	-	F9
0806	2	Port1 - Number of frames sent	0	4294967295	1	-	F9
0808	2	Port1 - Total bytes received	0	4294967295	1	-	F9
080A	2	Port1 - Total frames received	0	4294967295	1	-	F9
080C	2	Port1 - Number of broadcast frames received	0	4294967295	1	-	F9
080E	2	Port1 - Number of multicast frames received	0	4294967295	1	-	F9
0810	2	Port1 - Number of frames with CRC error	0	4294967295	1	-	F9
0812	2	Port1 - Number of oversized frames received	0	4294967295	1	-	F9
0814	2	Port1 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0816	2	Port1 - Number of jabber frames received	0	4294967295	1	-	F9
0818	2	Port1 - Number of collisions occurred	0	4294967295	1	-	F9
081A	2	Port1 - Number of late collisions occurred	0	4294967295	1	-	F9
081C	2	Port1 - Number of 64-byte frames rcvd/sent	0	4294967295	1	-	F9
081E	2	Port1 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0820	2	Port1 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
0822	2	Port1 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
0824	2	Port1 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0826	2	Port1 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
0828	2	Port1 - Number of Mac Error Packets	0	4294967295	1	-	F9
082A	2	Port1 - Number of dropped received packets	0	4294967295	1	-	F9
082C	2	Port1 - Number of multicast frames sent	0	4294967295	1	-	F9
082E	2	Port1 - Number of broadcast frames sent	0	4294967295	1	-	F9
0830	2	Port1 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
0832	2	Port2 - Number of bytes received	0	4294967295	1	-	F9
0834	2	Port2 - Number of bytes sent	0	4294967295	1	-	F9
0836	2	Port2 - Number of frames received	0	4294967295	1	-	F9
0838	2	Port2 - Number of frames sent	0	4294967295	1	-	F9
083A	2	Port2 - Total bytes received	0	4294967295	1	-	F9
083C	2	Port2 - Total frames received	0	4294967295	1	-	F9
083E	2	Port2 - Number of broadcast frames received	0	4294967295	1	-	F9
0840	2	Port2 - Number of multicast frames received	0	4294967295	1	-	F9
0842	2	Port2 - Number of frames with CRC error	0	4294967295	1	-	F9
0844	2	Port2 - Number of oversized frames received	0	4294967295	1	-	F9
0846	2	Port2 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0848	2	Port2 - Number of jabber frames received	0	4294967295	1	-	F9
084A	2	Port2 - Number of collisions occurred	0	4294967295	1	-	F9
084C	2	Port2 - Number of late collisions occurred	0	4294967295	1	-	F9
084E	2	Port2 - Number of 64-byte frames rcvd/sent	0	4294967295	1	-	F9
0850	2	Port2 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0852	2	Port2 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
0854	2	Port2 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9

Ad-dress	Qt-y	Description	Min	Max	St-ep	U-nit	Fo-rm-at
0856	2	Port2 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0858	2	Port2 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
085A	2	Port2 - Number of Mac Error Packets	0	4294967295	1	-	F9
085C	2	Port2 - Number of dropped received packets	0	4294967295	1	-	F9
085E	2	Port2 - Number of multicast frames sent	0	4294967295	1	-	F9
0860	2	Port2 - Number of broadcast frames sent	0	4294967295	1	-	F9
0862	2	Port2 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
		...					
144E	2	Port64 - Number of bytes received	0	4294967295	1	-	F9
1450	2	Port64 - Number of bytes sent	0	4294967295	1	-	F9
1452	2	Port64 - Number of frames received	0	4294967295	1	-	F9
1454	2	Port64 - Number of frames sent	0	4294967295	1	-	F9
1456	2	Port64 - Total bytes received	0	4294967295	1	-	F9
1458	2	Port64 - Total frames received	0	4294967295	1	-	F9
145A	2	Port64 - Number of broadcast frames received	0	4294967295	1	-	F9
145C	2	Port64 - Number of multicast frames received	0	4294967295	1	-	F9
145E	2	Port64 - Number of frames with CRC error	0	4294967295	1	-	F9
1460	2	Port64 - Number of oversized frames received	0	4294967295	1	-	F9
1462	2	Port64 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
1464	2	Port64 - Number of jabber frames received	0	4294967295	1	-	F9
1466	2	Port64 - Number of collisions occurred	0	4294967295	1	-	F9
1468	2	Port64 - Number of late collisions occurred	0	4294967295	1	-	F9
146A	2	Port64 - Number of 64-byte frames rcvd/sent	0	4294967295	1	-	F9
146C	2	Port64 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
146E	2	Port64 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
1470	2	Port64 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
1472	2	Port64 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
1474	2	Port64 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
1476	2	Port64 - Number of Mac Error Packets	0	4294967295	1	-	F9
1478	2	Port64 - Number of dropped received packets	0	4294967295	1	-	F9
147A	2	Port64 - Number of multicast frames sent	0	4294967295	1	-	F9
147C	2	Port64 - Number of broadcast frames sent	0	4294967295	1	-	F9
147E	2	Port64 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9

Application Example for the Modbus TCP Function

In the following example, you set up the device to respond to client requests. The prerequisite for this configuration is that the client device is set up with an IP address within the given range. The Write access function remains inactive for this example. When you activate the Write access function, the device allows port counters only to be reset. In the default setting the Modbus TCP and Write access functions are inactive.

The Modbus TCP function does not provide any authentication mechanisms. If the write access for Modbus TCP is activated, every client that can access the device using TCP/IP is capable of changing the settings of the device. As a result, incorrect device settings and potential network interruptions may occur.

NOTICE

UNAUTHORIZED ACCESS

Only activate the write access if you have taken additional measures (for example Firewall, VPN, etc.) to reduce possible unauthorized access.

Failure to follow these instructions can result in equipment damage.

Perform the following steps:

Step	Action
1	Navigate to **Device Security > Management Access > IP Access Restriction**.
2	Add a table row. To do this, click the ⊞ button.
3	Specify the IP address range in the table row where the Index column has the value **2**. To do this, enter the following values: • In the Address column: **10.17.1.0** • In the Netmask column: **255.255.255.248**
4	Verify that the checkbox in the Modbus TCP column is selected.
5	Activate the IP address range. To do this, select the checkbox in the Active column.
6	To apply the settings, click the ✓ button.
7	Navigate to the **Diagnostics > Status Configuration > Security Status**, **Global** tab.
8	Verify that the checkbox related to the parameter Modbus TCP active is selected.
9	Navigate to **Advanced > Industrial Protocols > Modbus TCP**. The standard Modbus TCP listening port, port **502**, is the default setting. However, when you wish to listen on another TCP port, enter the value for the listening port in the **TCP port** field.
10	Enable the Modbus TCP function. Select the **On** radio button in the Operation frame.
11	To apply the settings, click the ✓ button.
12	When you enable the Modbus TCP function, the Security Status function detects the activation and displays an alarm in the **Basic Settings > System** dialog, Security status frame.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`network management access add 2`	To add the entry for the address range in the network. Number of the next available index in this example: **2**.
`network management access modify 2 ip 10.17.1.0`	To specify the IP address.
`network management access modify 2 mask 29`	To specify the netmask.
`network management access modify 2 modbus-tcp enable`	To specify that the device gives Modbus TCP access to the device management.
`network management access operation`	To enable the IP access restriction.
`configure`	To change to the Configuration mode.
`security-status monitor modbus-tcp-enabled`	To specify that the device monitors the activation of the Modbus TCP server.

Command	Description
`modbus-tcp operation`	To enable the Modbus TCP server.
`modbus-tcp port <1..65535>`	To specify the TCP port for Modbus TCP communication (optionally). The default setting is port **502**.
`show modbus-tcp`	To display the Modbus TCP Server settings.

```
Modbus TCP/IP server settings
--------------------------
Modbus TCP/IP server operation................enabled
Write-access..................................disabled
Listening port................................502
Max number of sessions........................5
Active sessions...............................0
```

`show security-status monitor`	To display the security-status settings.

```
Device Security Settings
Monitor
----------------------------------
Password default settings unchanged..........monitored
...
Write access using Ethernet Switch Configurator is possible....monitored
Loading unencrypted configuration from ENVM...monitored
IEC 61850 MMS is enabled.....................monitored
Modbus TCP/IP server active..................monitored
```

`show security-status event`	To display detected security status events.

```
Time stamp              Event                       Info
--------------------    -----------------------    ------
2014-01-01 01:00:39   password-change(10)           -
....................................................
2014-01-01 01:00:39   ext-nvm-load-unsecure(21)     -
2014-01-01 23:47:40   modbus-tcp-enabled(23)        -
```

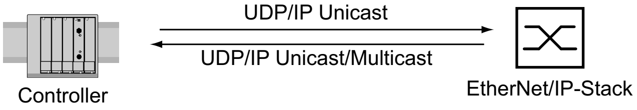
`show network management access rules 1`	To display the restricted management access rules for index **1**.

```
Restricted management access settings
-------------------------------------
Index........................................1
IP Address...................................10.17.1.0
Prefix Length................................29
HTTP.........................................yes
SNMP.........................................yes
Telnet.......................................yes
SSH..........................................yes
HTTPS........................................yes
IEC61850-MMS.................................yes
Modbus TCP/IP................................yes
Active.......................................[x]
```

EtherNet/IP Function

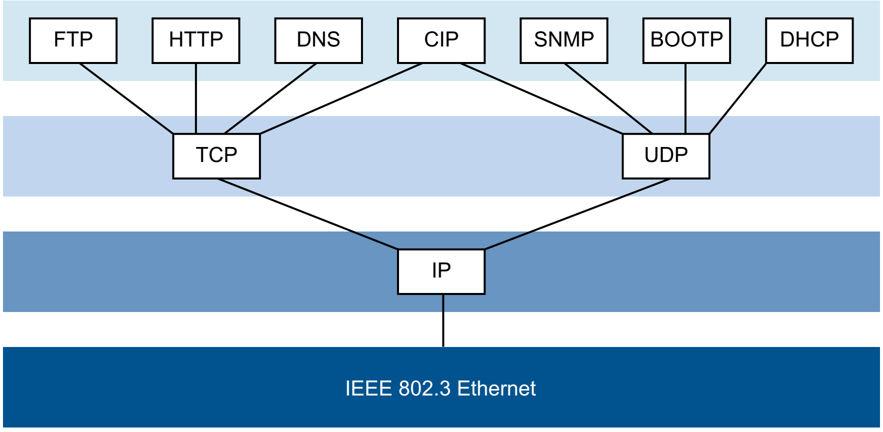
EtherNet/IP is an industrial communication protocol that is deployed worldwide and is maintained by the Open DeviceNet Vendor Association (ODVA). It is based on the protocols *TCP/IP* and *UDP/IP* over Ethernet. EtherNet/IP is supported by leading manufacturers, thus providing a wide base for effective data communication in the industry sector.

EtherNet/IP network:



EtherNet/IP adds the industry protocol CIP (Common Industrial Protocol) to the standard Ethernet protocols. EtherNet/IP implements CIP at the Session layer and above and adapts CIP to the specific EtherNet/IP technology at the Transport layer and below. In the case of automation applications, EtherNet/IP implements CIP on the application level. Therefore, EtherNet/IP is ideally suited to the industrial control technology sector.

IEEE 802.3 EtherNet/IP:



For further information on EtherNet/IP, see the ODVA website.

Integration Into a Control System

Perform the following steps:

Step	Action
1	Navigate to **Switching** > **IGMP Snooping** > **Global**. Verify that the IGMP Snooping function is enabled.
2	Navigate to **Advanced** > **Industrial Protocols** > **EtherNet/IP**. Verify that the EtherNet/IP function is enabled.
3	Navigate to **Advanced** > **Industrial Protocols** > **EtherNet/IP**.
4	To save the EDS as a ZIP archive on your PC, click Download. The ZIP archive contains the EtherNet/IP configuration file and the icon used to set up the controller to connect to the device.

EtherNet/IP Entity Parameters

The following paragraphs identify the objects and operations supported by the device.

Supported Operations

Overview of the supported EtherNet/IP requests for the objects instances:

Service Code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object	Base Switch Object
0x01 Get Attribute All	All attributes	All attributes	All attributes	All attributes	All attributes
0x02 Set Attribute All	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA)	Settable attributes (0x6, 0x9)	–	–
0x0e Get Attribute Single	All attributes	All attributes	All attributes	All attributes	All attributes
0x10 Set Attribute Single	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA, 0x64)	Settable attributes (0x6, 0x9, 0x65, 0x67, 0x68, 0x69, 0x6C)	Settable attributes (0x5, 0x7)	–
0x05 Reset	Parameter (0x0, 0x1)	–	–	–	–
0x35 Save Configuration Vendor specific	–	–	–	Save switch configuration	–
0x36 Mac Filter Vendor specific	–	–	–	Add MAC filter STRUCT of: • USINT VlanId • ARRAY of: 6 USINT Mac • DWORD PortMask	–

Identity Object

The device supports the identity object (*Class Code 0x01*) of EtherNet/IP. The Schneider Electric manufacturer ID is 634. Schneider Electric uses the ID 44 (0x2C) to indicate the product type "Managed Ethernet Switch".

Instance attributes (only instance 1 is available):

Id	Attribute	Access rule	Data type	Description
0x1	Vendor ID	Get	UINT	Schneider Electric634
0x2	Device Type	Get	UINT	Managed Ethernet Switch 44 (0x2C) (0x2C)
0x3	Product Code	Get	UINT	Product Code: mapping is defined for every device type
0x4	Revision	Get	STRUCT of: • USINT Major • USINT Minor	Revision of the EtherNet/IP implementation, 2.1.
0x5	Status	Get	WORD	Support for the following Bit status only:
				0: Owned (constantly 1)
				2: Configured (constantly 1)
				4: Extend Device Status
				5: 0x3: No I/O connection established
				6: 0x7: At least one I/O connection established, all in idle mode.
				7:
0x6	Serial number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
0x7	Product name	Get	SHORT-STRING	Displayed as "Schneider Electric" + product family + product ID + software variant.

TCP/IP Interface Object

The device supports only Instance 1 of the TCP/IP Interface Object (*Class Code 0xF5*) of EtherNet/IP.

Depending on the write access configuration, the device stores all settings in its flash memory. Saving the settings can take up to 10 seconds. If the saving process is interrupted for example, due to an inoperable power supply, the device may become inoperable.

> **NOTE:** When a configuration change is made, the device responds to the **Get Request** with a **Response**, even though the settings may not yet be fully saved to flash memory.

Class attributes:

Id	Attribute	Access rule	Data type	Description
0x1	Revision	Get	UINT	Revision of this object: 3
0x2	Max Instance	Get	UINT	Maximum instance number: 1
0x3	Number of instance	Get	UINT	Number of object instances added: 1

Attributes of Instance 1:

Id	Attribute	Access rule	Data type	Description	
0x1	Status	Get	DWORD	0:	Interface Status (0=Interface not configured, 1=Interface contains valid config)
				6:	ACD status (default 0)
				7:	ACD error (default 0)
0x2	Interface Capability flags	Get	DWORD	0:	BOOTP Client
				1:	DNS Client
				2:	DHCP Client
				3:	DHCP-DNS Update
				4:	Configuration settable (within CIP) Other bits reserved (0)
				7:	ACD capable (0=not capable, 1= capable)
0x3	Config Control	Set/Get	DWORD	• 0: 0x0=using stored config • 1: 0x1=using BOOTP • 2: 0x 2=using DHCP • 3: One device uses DNS for name lookup (constantly 0 because it is unsupported) • 4: Other bits reserved (0)	
0x4	Physical Link Object	Get	STRUCT of: • UINT PathSize • EPATH Path	Path to the Physical Link Object, constantly {0x20, 0xF6, 0x24, 0x01} describing instance 1 of the Ethernet Link Object.	
0x5	Interface Configuration	Set/Get	STRUCT of: • UDINT IpAddress • UDINT Netmask • UDINT GatewayAddress • UDINT NameServer1 • UDINT NameServer2 • STRING DomainName	IP Stack Configuration (IP address, Netmask, Gateway, 2 Name servers (DNS, if supported) and the domain name).	
0x6	Hostname	Set/Get	STRING	Hostname (for DHCP DNS Update)	
0x7	Safety Network Number			Unsupported	
0x8	TTL Value	Get/Set	USINT	Time to live value for IP multicast packets Range 1..255 (default 1)	
0x9	Mcast Config	Get/Set	STRUCT of: • USINT AllocControl • USINT reserved • UINT NumMcast • UDINT McastStartAddr	Alloc Control = 0 Number of IP multicast addresses = 32 Multicast start address = 239.192.1.0	
0xA	Selected Acd	Get/Set	BOOL	0=ACD disable 1=ACD enable (default)	
0xB	Last Conflict Detected	Get	STRUCT of: • USINT AcdActivity • ARRAY of 6 USINT RemoteMac: • ARRAY of: 28 USINT ArpPdu	ACD Diagnostic Parameters	

Schneider Electric extensions to the TCP/IP Interface Object:

Id	Attribute	Access rule	Data type	Description
0x64	Cable Test	Set/Get	STRUCT of: • USINT Interface • USINT Status	Interface Status (1=Active, 2=Success, 3=Error, 4= Uninitialized)
0x65	Cable Pair Size	Get	USINT	Size of the Cable Test Result STRUCT of: 2 Pair for 100BASE 4 Pair for 1000BASE

0x66	Cable Test Result	Get	STRUCT of:
			• USINT Interface
			• USINT CablePair
			• USINT CableStatus
			• USINT CableMinLength
			• USINT CableMaxLength
			• USINTCableFailureLocation
				100BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}
				1000BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair3, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair4, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}

Ethernet Link Object

The information in the following two tables is part of the Ethernet Link Object. To access the information, use the following values:

- Class(####)
- Instance(###)
- Attribute(#)

For example, the *class*, *instance*, and *attribute* values to access information for the utilization alarm using an explicit message are:

- Class = 0xF6
- Instance = 1
- Attribute = 6

Instance attributes and Schneider Electric extensions to the Ethernet Link Object:

Id	Attribute	Access rule	Data type	Description	
Instance attributes					
0x1	Interface Speed	Get	UDINT	Used interface speed in Mbit/s (10, 100, 1000, …). 0 is used when the speed has not been determined or is invalid because of detected errors.	
0x2	Interface Flags	Get	DWORD	Interface Status Flags:	
				0:	Link State (0=No link, 1=Link)
				1:	Duplex mode (0=Half, 1=Full)
				2:	Auto-negotiation Status 0x0=Auto-negotiation in progress 0x1=Unsuccessful auto-negotiation detected error 0x2=Unsuccessful but speed detected 0x3=Auto-negotiation success 0x4=No Auto-negotiation
				3:	
				4:	
				5:	Manual configuration require reset (constantly 0 because it is not needed)
				6:	Hardware error
0x3	Physical Address	Get	ARRAY of: 6 USINT	MAC address of physical interface	
0x4	Interface Counters	Get	STRUCT of: • UDINT MibIICounter1 • UDINT MibIICounter2 • …	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors	
0x5	Media Counters	Get	STRUCT of: • UDINT EthernetMib Counter1 • UDINT EthernetMib Counter2 • …	Detected errors: Alignment, FCS, single collision, multiple collision, SQE Test, deferred transmissions, late collisions, excessive collisions, MAC TX, carrier sense, frame too long, MAC RX	
0x6	Interface Control	Get/Set	STRUCT of:		Control Bits:
			WORD ControlBits	0:	Auto-negotiation enable/disable (0=disable, 1=enable)
				1:	Duplex mode (0=Half, 1=Full), if Auto-negotiation disabled
			UINT ForcedInterface Speed	Interface speed in Mbit/s: 10,100,…, if Auto-negotiation disabled	
0x7	Interface type	Get	USINT	Type of interface: 0: Undefined interface type 1: The interface is internal 2: Twisted-pair 3: Optical fiber	
0x8	Interface state	Get	USINT	Present state of the interface: 0: Undefined interface state 1: The interface is enabled 2: The interface is disabled 3: The interface is testing	

Id	Attribute	Access rule	Data type	Description
0x9	Admin State	Set/Get	USINT	Administrative state: 1: Enable the interface 2: Disable the interface
0xA	Interface label	Get	SHORT-STRING	Human readable ID
Schneider Electric extensions to the Ethernet Link Object				
0x64	Ethernet Interface Index	Get	USINT	Interface/Port Index (ifIndex out of MIBII)
0x65	Port Control	Get/Set	DWORD	0: Link state (0=link down, 1=link up) 1: Link admin state (0=disabled, 1=enabled) 8: Access violation alarm (read-only) 9: Utilization alarm (read-only)
0x66	Interface Utilization	Get	USINT	The existing Counter out of the private MIB hm2IDiagfaceUtilization is used. Utilization in percentage (Unit 1%=100, %/100). RX Interface Utilization.
0x67	Interface Utilization Alarm Upper Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmUpperThreshold can be accessed. Utilization in percentage (Unit 1% =100). RX Interface Utilization Upper Limit.
0x68	Interface Utilization Alarm Lower Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage (Unit 1% =100). RX Interface Utilization Lower Limit.
0x69	Broadcast limit	Get/Set	USINT	Broadcast limiter Service (Egress BC-Frames limitation, 0=disabled), Frames/ second
0x6A	Ethernet Interface Description	Get/Set	STRING	Interface/Port Description (from MIB II ifDescr), for example "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX" or "unavailable", max. 64 Bytes.

Id	Attribute	Access rule	Data type	Description	
0x6B	Port Monitor	Get/Set	DWORD	0:	Link Flap (0=Off, 1=On)
				1:	CRC/Fragment (0=Off, 1=On)
				2:	Duplex Mismatch (0=Off, 1=On)
				3:	Overload-Detection (0=Off, 1=On)
				4:	Link-Speed/ Duplex Mode (0=Off, 1=On)
				5:	Deactivate port action (0=Off, 1=On)
				6:	Send trap action (0=Off, 1=On)
				7:	Active Condition (displays which condition caused an action to occur) 00001$_B$: Link Flap 00010$_B$: CRC/Fragments 00100$_B$: Duplex Mismatch 01000$_B$: Overload-Detection 10000$_B$: Link-Speed/ Duplex mode
				8:	
				9:	
				10:	
				11:	
				12:	Reserved (constantly 0)
				13:	Reserved (constantly 0)
				14:	Reserved (constantly 0)
				15:	Reserved (constantly 0)
0x6C	Quick Connect	Get/Set	USINT	Quick Connect on the interface (0=Off, 1=On) If you enable Quick Connect, the device sets the port speed to 100FD, disables auto-negotiation, and Spanning Tree on the interface.	
0x6D	SFP Diagnostics	Get	STRUCT of: • STRING ModuleType in °C • SHORT-STRING SerialNumber • USINT Connector • USINT Supported • DINT Temperature • DINT TxPower in mW • DINT RxPower in mW • DINT RxPower in dBm • DINT TxPower in dBm		

Assignment of ports to Ethernet Link Object Instances:

Ethernet Port	Ethernet Link Object Instance
Controller	1
1	2
2	3
3	4
4	5
…	…

NOTE: The number of ports depends on the type of hardware used. The Ethernet Link Object only exists, if the port is connected.

Switch Agent Object

The device supports the Schneider Electric specific Ethernet Switch Agent Object (*Class Code 0x95*) for the device settings and information parameters with Instance 1.

Class attributes

Id	Attribute	Access rule	Data type	Description	
0x1	Switch Status	Get	DWORD	0:	Like the signal contact, the value indicates the Device Overall state (0=ok, 1=error detected)
				1:	Device Security Status (0=ok, 1=error detected)
				2:	Power Supply 1 (0=ok, 1=error detected)
				3:	Power Supply 2 (0=ok, 1=error detected or absent)
				4-5:	Reserved
				6:	Signal Contact 1 (0=closed, 1=open)
				7:	Signal Contact 2 (0=closed, 1=open or absent)
				8:	Reserved
				9:	Temperature (0=ok, 1=error detected)
				10:	Module removed (1=removed)
				11:	EAM removed (1=removed)
				12:	EAM-SD removed (1=removed)
				13-22:	Reserved
				23:	MRP (0=disabled, 1=enabled)
				24:	Reserved
				25:	Reserved
				26:	RSTP (0=disabled, 1=enabled)
				27:	LAG (0=disabled, 1=enabled)
				28:	Reserved
				29-30	Reserved
				31:	Connection Error (1=error detected)
0x2	Switch Temperature	Get	STRUCT of: • INT TemperatureF • INT TemperatureC	in °F in °C	
0x3	Reserved	Get	UDINT	Reserved (constantly 0)	
0x4	Switch Max Ports	Get	UINT	Maximum number of Ethernet Switch Ports	

Id	Attribute	Access rule	Data type	Description	
0x5	Multicast Settings (IGMP Snooping)	Get/Set	WORD	0:	IGMP Snooping (0=disabled, 1=enabled)
				1:	IGMP Querier (0=disabled, 1=enabled)
				2:	IGMP Querier Mode (read-only) (0=Non-Querier, 1=Querier)
				3:	
				4:	IGMP Querier Packet Version Off=0 IGMP Querier disabled V1=1 V2=2 V3=3
				5:	
				6:	
				7:	
				8:	Treatment of undefined multicasts: 0=Send To All Ports 2=Discard
				9:	
				10:	
0x6	Switch Existing Ports	Get	ARRAY of: DWORD	Bitmask of existing switch ports Per bit starting with Bit 0 (=Port 1) (0=Port not available, 1=Port existing) Array (bit mask) size is adjusted to the size of maximum number of switch ports (for max. 28 Ports 1 DWORD is used)	
0x7	Switch Port Control	Get/Set	ARRAY of: DWORD	Bitmask Link Admin Status switch ports Per bit starting with Bit 0 (=Port 1) (0=Port enabled, 1=Port disabled) Array (bit mask) size is adjusted to the size of maximum number of Switch ports (for max. 28 Ports 1 DWORD is used)	
0x8	Switch Ports Mapping	Get	ARRAY of: USINT	Instance number of the Ethernet-Link-Object Starting with Index 0 (=Port 1) All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N, maximum number of ports). When the entry is 0, the Ethernet Link Object for this port does not exist	
0x9	Switch Action Status	Get	DWORD	Status of the last executed action (for example config save, software update, etc.)	
				0:	Flash Save Configuration In Progress/ Flash Write In Progress
				1:	Flash Save Configuration error detected/ Flash Write error detected
				4:	Configuration changed (configuration not in sync. between running configuration

The Schneider Electric specific Ethernet Switch Agent Object provides you with the additional vendor specific service, with the *Service Code 0x35* for saving the device settings. When you send a request from your PC to save the device settings, the device sends a reply after saving the settings in the flash memory.

Base Switch Object

The Base Switch object provides the CIP application-level interface to basic status information for a managed Ethernet switch (revision 1).

Only Instance 1 of the Base Switch (*Class Code 0x51*) is available.

Instance attributes:

Id	Attribute	Access rule	Data type	Description
0x1	Device Up Time	Get	UDINT	Time since the device powered up
0x2	Total port count	Get	UDINT	Number of physical ports
0x3	System Firmware Version	Get	SHORT-STRING	Human readable representation of System Firmware Version
0x4	Power source	Get	WORD	Status of switch power source
0x5	Port Mask Size	Get	UINT	Number of DWORD in port array attributes
0x6	Existing ports	Get	ARRAY of: DWORD	Port Mask
0x7	Global Port Admin State	Get	ARRAY of: DWORD	Port Admin Status
0x8	Global Port link Status	Get	ARRAY of: DWORD	Port Link Status
0x9	System Boot Loader Version	Get	SHORT-STRING	Readable System Firmware Version
0xA	Contact Status	Get	UDINT	Switch Contact Closure
0xB	Aging Time	Get	UDINT	Range 10..1000000 · 1/10 seconds (default 300) 0=Learning off
0xC	Temperature C	Get	DINT	Switch temperature in degrees Celsius
0xD	Temperature F	Get	DINT	Switch temperature in degrees Fahrenheit

Message Router

The Message Router object *(Class Code 0x20)* distributes *Explicit Request* messages to the appropriate handler object.

Class attributes:

Id	Attribute	Access rule	Data type	Description
1	Revision	Get	UINT	Revision: 1
2	Largest Instance Number	Get	UINT	Largest instance number: 1
3	Number of Instances Existing	Get	UINT	Number of instances existing: 1
4	Optional Attribute List	Get	ARRAY of: BYTES	Optional attribute list: 0 Unsupported for Get_single service
5	Optional Service List	Get	ARRAY of: BYTES	Optional Service List: 0 Unsupported for Get_single service
6	Maximum ID Number Class Attributes	Get	UINT	Maximum ID Number Class Attributes: 7
7	Maximum ID Number Instance Attributes	Get	UINT	Maximum ID Number Instance Attributes: 0

Assembly

The Assembly object *(Class Code 0x04)* binds attributes of multiple objects. This property allows the device to send or receive data to or from any object over a single connection. You can use Assembly objects to bind *Input* or *Output* data. The terms *Input* and *Output* are specified from the viewpoint of the network. *Input* produces data on the network and *Output* consumes data from the network.

Supported instances

Instance	**Description**	**Service**
1	POWER_LINK_ASSEMBLY	Get_single
100	INPUT_ASSEMBLY_NUM	Get_single
150	OUTPUT_ASSEMBLY	Get_single/Set_single
151	CONFIG_ASSEMBLY_NUM	Get_single/Set_single
152	HEARBEAT_INPUT_ONLY_ASSEMBLY	Get_single/Set_single
153	HEARBEAT_LISTEN_ONLY_ASSEMBLY	Get_single/Set_single
154	EXPLICT_ASSEMBLY	Get_single/Set_single

Class attributes:

Id	**Attribute**	**Access rule**	**Data type**	**Description**
1	Revision	Get	UINT	Revision: 2
2	Largest Instance Number	Get	UINT	Largest instance number: 154
3	Number of Instances Existing	Get	UINT	Number of instances existing: 7
4	Optional Attribute List	-	-	Unsupported
5	Optional Service List	-	-	Unsupported
6	Maximum ID Number Class Attributes	Get	UINT	Maximum ID Number Class Attributes: 7
7	Maximum ID Number Instance Attributes	Get	UINT	Maximum ID Number Instance Attributes: 4

Instance attributes:

Id	**Attribute**	**Access rule**	**Data type**	**Description**
3	Data	Get	ARRAY of: BYTES	-
4	Size	Get	UINT	Number of bytes in Attribute 3

Connection Manager

The Connection Manager Class (*Class Code 0x06*) allocates and manages the internal resources associated with both *I/O* and *Explicit Messaging* connections.

Class attributes:

Id	Attribute	Access rule	Data type	Description
1	Revision	Get	UINT	Revision: 1
2	Largest Instance Number	Get	UINT	largest instance number: 1
3	Number of Instances Existing	Get	UINT	Number of instances existing: 1
4	Optional Attribute List	-	-	Unsupported
5	Optional Service List	-	-	Unsupported
6	Maximum ID Number Class Attributes	Get	UINT	Maximum ID Number Class Attributes: 7
7	Maximum ID Number Instance Attributes	Get	UINT	Maximum ID Number Instance Attributes: 14

QoS Object

The QoS object (0x48) provides sending EtherNet/IP messages with non-zero DiffServ code points (DSCP). The QoS object supports one instance.

Class attributes:

Id	Attribute	Access rule	Data type	Description
0x1	Revision	Get	UINT	Revision of this object: 1
0x2	Max Instance	Get	UINT	Maximum instance number: 1
0x3	Number of instance	Get	UINT	Number of object instances added: 1
0x4	Optional Attribute List	-	-	Unsupported
0x5	Optional Service List	-	-	Unsupported
0x6	Maximum ID Number Class Attributes	Get	UINT	Maximum ID Number Class Attributes: 7
0x7	Maximum ID Number Instance Attributes	Get	UINT	Maximum ID Number Instance Attributes: 8

Instance attributes:

Id	Attribute	Access rule	Data type	Description
0x1	802.1Q TagEnable	-	-	Unsupported
0x2	DSCP PTP Event	-	-	Unsupported
0x3	DSCP PTPGeneral	-	-	Unsupported
0x4	DSCP Urgent	Get/Set	USINT	DSCP value for CIP transport class 0/1 Urgent priority messages. (default 55)
0x5	DSCP Scheduled	Get/Set	USINT	DSCP value for CIP transport class 0/1 Scheduled priority messages. (default 47)
0x6	DSCP High	Get/Set	USINT	DSCP value for CIP transport class 0/1 High priority messages. (default 43)
0x7	DSCP Low	Get/Set	USINT	DSCP value for CIP transport class 0/1 Low priority messages. (default 31)
0x8	DSCP Explicit	Get/Set	USINT	DSCP value for CIP explicit messages (transport class 2/3 and UCMM) and all other EtherNet/IP encapsulation messages. (default 27)

Services, Connections and I/O Data

The device supports the following connection types and parameters.

Settings for integrating a new module:

Setting	I/O connection	Input only	Listen only
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/ Program
IP address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	100	100	100
Input Size	32	32	32
Output Assembly Instance	150	152	153
Output Size	32	0	0
Configuration Assembly Instance	151	151	151
Data Size	10	10	10

Device I/O data structure:

I/O Data	Value (data types and sizes to be defined)	Direction	Size [4]
Device Status	Bitmask (see Switch Agent Attribute 0x1)	Input	DWORD
Link Status	Bitmask, 1 Bit per port (0=No link, 1=Link up)	Input	DWORD
Output Links Admin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, for example for controller access port. (0=Port enabled, 1=Port disabled)	Input	DWORD
Utilization Alarm [5]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Access Violation Alarm [6]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Multicast Connections	Integer, number of connections	Input	DINT
TCP/IP Connections	Integer, number of connections	Input	DINT
Quick Connect Mask	Bitmask (1 Bit per port) (0=Quick Connect disabled, 1=Quick Connect enabled)	Input	DINT
Link Admin State	Bitmask, 1 Bit per port (0=Port enabled, 1=Port disabled)	Output	DWORD

Mapping of the data types to bit sizes:

Object type	Bit size
BOOL	1 bit
DINT	32 bit
DWORD	32 bit
SHORT-STRING	max. 32 bytes
STRING	max. 64 bytes
UDINT	32 bit
UINT	16 bit
USINT	8 bit
WORD	16 bit

OPC UA Server

The *Open Platform Communications United Architecture* (*OPC UA*) is a protocol for industrial communication, and describes a variety of *OPC UA* information models. The *OPC UA* protocol is a standardized protocol for the exchange of data in the industrial automation space and in other industries.

The *OPC UA* protocol provides a very flexible and adaptable mechanism for transferring the data between industrial automation equipment, monitoring devices, and sensors. The *OPC UA* protocol uses a standard interface, for example, *HTTPS* that makes the protocol simple to integrate into existing

[4] The default size of the port bit masks is 32 bits (DWORD). For devices with more than 28 ports the port bit masks have been extended to n * DWORD.

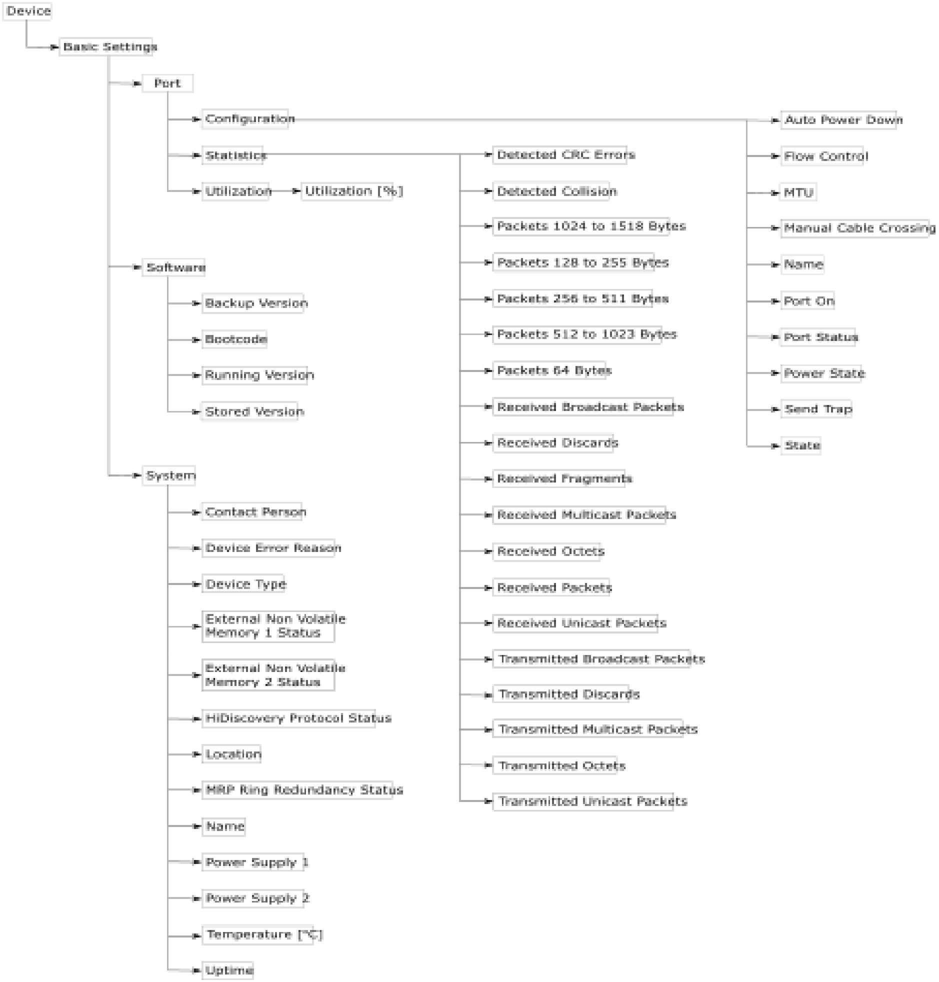
[5] You specify the utilization alarm settings in the **Basic Settings > Port**, **Ingress Utilization** tab. The upper threshold value is the limit, where the alarm condition becomes active. The lower threshold value is the limit, where an active alarm condition becomes inactive.

[6] You specify the Access Violation alarm settings in the **Network Security > Port Security** dialog. The upper threshold value is the limit, where the alarm condition becomes active. The lower threshold value is the limit, where an active alarm condition becomes inactive.

management systems. The device operating as an *OPC UA* server transmits the data of the connected end devices, ranging from simple uptime status to large amounts of complex industrial data.

The following figure displays the *OPC UA* information model data of the connected end devices available to the *OPC UA* client.

OPC UA information model:



Objects in the OPC UA information model:

Object	Description
Power save	Specifies how the port behaves when no cable is connected.
Port on	Activates/deactivates the port.
Power state	Specifies if the port is physically switched on or off when you deactivate the port with the Port on function.
State	Displays if the port is physically enabled or disabled.
Port status	Displays the link status of the port.

Object values in the OPC UA information model:

Object	Val-ue	Description
Device Error Reason	1	None
	2	Power supply
	3	Link error
	4	Temperature
	5	Fan interruption
	6	Module removal
	7	External non-volatile memory removal
	8	External non-volatile memory not in synchronization
	9	Ring redundancy
External non-volatile Memory 1 Status	1	Not present
	2	Removed
	3	Ok
	4	Out of memory
	5	Generic error
External non-volatile Memory 2 Status	1	Not present
	2	Removed
	3	Ok
	4	Out of memory
	5	Generic error
HiDiscovery Protocol Status	1	Enabled
	2	Disabled
MRP Ring Redundancy Status	1	Available
	2	Not available
Power Supply 1	1	Present
	2	Inoperable
	3	Not installed
	4	Undefined
Power Supply 2	1	Present
	2	Inoperable
	3	Not installed
	4	Undefined
Auto Power Down	1	Auto power down
	2	No power save
	3	Energy efficient ethernet
	4	Unsupported
Flow Control	1	Enabled
	2	Disabled
Manual Cable Crossing	1	Medium dependent interface
	2	Medium dependent interface crossover
	3	Auto medium dependent interface crossover
	4	Unsupported

Object	Value	Description
Port On	1	Up
	2	Down
	3	Testing
Power State	1	Enabled
	2	Disabled
Send Trap	1	Enabled
	2	Disabled
State	1	Up
	2	Down
Port Status	1	Up
	2	Down
	3	Testing
	4	Undefined
	5	Dormant
	6	Not present
	7	Lower layer down

The device operating as an *OPC UA* server processes the *OPC UA* information model data and transmits it securely to the *OPC UA* client application. The *OPC UA* server and *OPC UA* client communicate through a session.

The device operating as an *OPC UA* server shares the monitored data of the *OPC UA* information model. The user of the *OPC UA* client selects the items to be monitored in the *OPC UA* client application from a list of the IEC variables. The *OPC UA* client application requests the *OPC UA* information model data from the device operating as an *OPC UA* server using the specified *OPC UA* user account data.

The device sets up an *OPC UA* session by first negotiating the policy for a secure connection. Over this secure connection, the *OPC UA* client sends the login credentials of the *OPC UA* user account. The *OPC UA* server in the device then authenticates the *OPC UA* client. When the login credentials are valid, the device grants the *OPC UA* client access to its OPC UA Server function.

The device offers a role-based authentication and encryption concept to specifically control the access to its *OPC UA* server. The *OPC UA* client can use commands and functions associated with the *OPC UA* user account set up in the device.

Enabling the *OPC UA* Server

In the default setting, the OPC UA Server function is disabled. The **Advanced > Industrial Protocols > OPC UA Server** dialog allows the OPC UA Server function to be enabled. You can also specify the max. number of simultaneous *OPC UA* sessions. In the default setting, the values for the **Listening port** and **Sessions (max.)** fields are already specified. You specify the authentication and encryption protocol for *OPC UA* users at global level.

Perform the following steps:

Step	Action
1	Navigate to **Advanced > Industrial Protocols > OPC UA Server**.
2	Enable the OPC UA Server function. Select the **On** radio button in the Operation frame.
3	To apply the settings, click the ✓ button.
4	In the **Listening port** field, change the TCP port number, if necessary.
5	In the **Sessions (max.)** field, change the number of *OPC UA* sessions that can be established simultaneously, if necessary.
6	In the **Security policy** field, select the authentication and encryption protocol.
7	To apply the settings, click the ✓ button. The dialog displays the To apply the changes, restart the OPC/UA server. Restart now? window.
8	To apply the settings, click **Yes**.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`opc-ua operation`	To enable the OPC UA Server server.
`opc-ua port <1..65535>`	To change the TCP port number, if necessary.
`opc-ua sessions <1..5>`	To specify the number of *OPC UA* connections that can be established simultaneously.
`opc-ua security-policy none | basic128rsa15 | basic256 | basic256sha256`	To specify the authentication and encryption protocol.
`show opc-ua global`	To display the *OPC UA* Server settings.

```
IEC62541 - OPC/UA server settings
--------------------------
IEC62541 - OPC/UA server operation..........enabled
Listening port..............................4840
Number of concurrent sessions...............5
Configured security-policy..................none
```

Setting Up an *OPC UA* User Account

The device allows the *OPC UA* to manage user accounts required to access the device using a *OPC UA* client application. Every *OPC UA* client user requires an active *OPC UA* user account to gain access to the *OPC UA* server of the device.

In the following example, you set up an *OPC UA* user account for the *OPC UA* client user **USER** which has read access. The user **USER** is authorized to monitor the *OPC UA* information model data.

Perform the following steps:

Step	Action
1	Navigate to **Advanced > Industrial Protocols > OPC UA Server**.
2	Click the ⊞ button. The dialog displays the Create window.
3	Enter the name **USER** in the **User name** field.
4	Click **OK**.
5	In the **Password** field, enter a password of at least 6 characters. In this example, you give the user account the password **SECRET**.
6	In the Access role column, select the readOnly item.
7	To apply the settings, click the ✓ button. The dialog displays the To apply the changes, restart the OPC/UA server. Restart now? window.
8	To apply the settings, click **Yes**. The dialog displays the *OPC UA* user accounts that are set up.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users add USER`	To add the *OPC UA* user account `USER`.

`opc-ua users modify USER password`
`Enter NEW password: ****** (SECRET)`
`Confirm NEW password: ****** (SECRET)`
	To enter and confirm the password `SECRET` for the *OPC UA* user account `USER`. Enter a password of at least 6 characters.

`opc-ua users modify USER access-role read-only`	To assign the access role **readOnly** to the *OPC UA* user account `USER`.
`opc-ua users enable USER`	To activate the user account `USER`.
`show opc-ua users`	To display the user accounts that are set up.

```
User Name                  Access-Role      Status
-------------------------- ---------------- ------
user                       read-only        [x]
```

NOTE: When you set up a new *OPC UA* user account, set the password.

Deactivating an *OPC UA* User Account

After you deactivate the *OPC UA* user account, the user cannot access the device using the OPC UA Server function. Deactivating an *OPC UA* user account allows the account settings to be saved and reused in the future.

Perform the following steps:

Step	Action
1	Navigate to **Advanced > Industrial Protocols > OPC UA Server**. The dialog displays the *OPC UA* user accounts that are set up.
2	In the table row for the relevant *OPC UA* user account, clear the checkbox in the Active column.
3	To apply the settings, click the ✓ button. The dialog displays the To apply the changes, restart the OPC/UA server. Restart now? window.
4	To apply the settings, click **Yes**.

Execute the following commands:

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><code>enable</code></td><td>To change to the Privileged EXEC mode.</td></tr>
<tr><td><code>configure</code></td><td>To change to the Configuration mode.</td></tr>
<tr><td><code>opc-ua users disable USER</code></td><td>To disable the user account <code>USER</code>.</td></tr>
<tr><td><code>show opc-ua users</code></td><td>To display the user accounts that are set up.</td></tr>
<tr><td colspan="2"><pre>User Name   Access-Role   Status
-------------------------- ------------- ------
user   read-only   [ ]</pre></td></tr>
<tr><td><code>save</code></td><td>To save the settings in the non-volatile memory (<b>nvm</b>) in the <b>Selected</b> configuration profile.</td></tr>
</table>

Deleting an *OPC UA* User Account

To permanently deactivate the *OPC UA* user account settings, you delete the *OPC UA* user account.

Perform the following steps:

Step	Action
1	Navigate to **Advanced > Industrial Protocols > OPC UA Server**. The dialog displays the *OPC UA* user accounts that are set up.
2	Select the table row of the relevant *OPC UA* user account.
3	Click the ✖ button.
4	To apply the settings, click the ✓ button. The dialog displays the To apply the changes, restart the OPC/UA server. Restart now? window.
5	To apply the settings, click **Yes**.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`opc-ua users delete USER`	To delete the user account `USER`.
`show opc-ua users`	To display the user accounts that are set up.

`User Name                  Access-Role   Status`
`-------------------------- ------------- ------`	

`save`	To save the settings in the non-volatile memory (**nvm**) in the **Selected** configuration profile.

Service Discovery

Service Discovery is part of a series of technologies summarized by the term Zero-configuration networking (zeroconf). Service Discovery uses multicast DNS (mDNS) and DNS service discovery (DNS-SD) to advertise the services offered by the device to other devices in the network that request the service. The device supports the ITxPT Module Inventory service.

Devices that support Service Discovery can automatically discover the available services on the network without having information about which devices are available. In public transportation, for example, such devices can be ticketing systems, passenger information systems, or vehicle tracking systems.

Devices that subscribe to the services will detect a new device as soon as you connect it to the network, and read its service data. For example, when you install a ticketing system in the network of a public transportation vehicle, the ticketing system needs to communicate with the existing passenger information system to deliver real-time updates on ticket sales and availability.

ITxPT Module Inventory

The ITxPT Module Inventory service is part of the Information Technology for Public Transport (ITxPT) specification.

The intended use of the ITxPT Module Inventory service is module inventory in networks of vehicles. The ITxPT Module Inventory service allows devices subscribing to the service automatically to inventory the modules installed in the on-board IP network of vehicles. Modules in the sense of ITxPT might be other Schneider Electric devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system. The service allows collection of information about the modules and monitor their status.

The device provides the information through *SRV records* and *TXT records*.

- The *SRV record* contains the location.

- The device provides the *TXT record* through mDNS. The *TXT record* contains information about the service.
  - `version`

    Version of the related ITxPT specification release

    Example: `2.1.2`
  - `type`

    Short name of the device type

    Example: `MESW (Managed Ethernet Switch)`
  - `model`

    Name of the device

    For example, the product code

    Example: `MCSESM`
  - `manufacturer`

    Manufacturer of the device

    Example: `Schneider Electric SE`
  - `serialnumber`

    Serial number of the device

    Example: `942287999020501939`
  - `softwareversion`

    Software version installed on the device

    Example: `MCSESM Release 99.9.002025-09-20 06:33`
  - `hardwareversion`

    Hardware version of the device

    Example: `0202`
  - `macaddress`

    MAC address of the device in hexadecimal format

    Example: `CF:DA:98:63:9D:F6`
  - `status`

    Integer containing the last detected error

    The value `0` means: No error detected.

    Example: `C0FFFFFFFFF3FFFF01FCFFFF FFFFFFFF`
  - `xstatus`

    Detailed device status

    For example, the status of the ports participating in the ITxPT Module Inventory service

    Example: `C0FFFFFFFFF3FFFF01FCFFFF FFFFFFFF`
  - `services`

    List of available services on the device

    For example, the ITxPT Module Inventory service

    Example: `inventory`

The device transmits the *TXT record* once in the following cases:

- After an mDNS query containing the address _itxpt_socket._tcp.local

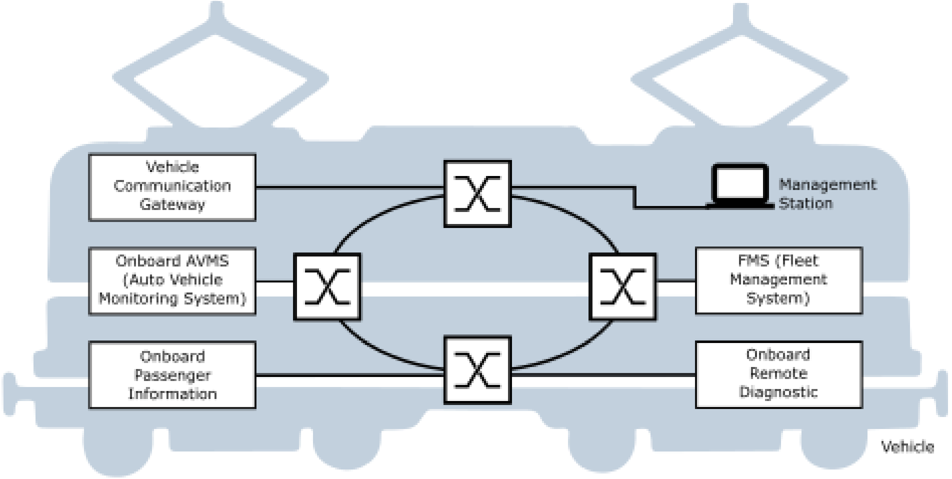
  The device transmits the *TXT record* in response to multicast or unicast requests in the network for services offered by the device.

- Without a request
  - As soon as the Service Discovery function and the ITxPT Module Inventory service are enabled. See the Operation frame.
  - If the Service Discovery function and the ITxPT Module Inventory service are enabled, and the device detects changes regarding the global status or the port status of other devices in the network. Other devices might be other Schneider Electric devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system.

Application Example

The following example illustrates a typical use case in the field of public transportation. The vehicle on-board network contains, in addition to switches and the PC, the on-board passenger information system, the on-board remote diagnostic system, and other devices typical for this application.

Example for ITxPT Module Inventory


Vehicle Communication Gateway
Management Station
Onboard AVMS (Auto Vehicle Monitoring System)
FMS (Fleet Management System)
Onboard Passenger Information
Onboard Remote Diagnostic
Vehicle

Enabling the Service Discovery Function on the Device

Enable the Service Discovery function on every switch in the on-board network. Simultaneously, the device activates the ITxPT Module Inventory service to monitor the link status or the PoE status of the device.

Perform the following steps:

Step	Action
1	Enable the Service Discovery function and activate the ITxPT Module Inventory service on the device. Select the **On** radio button in the Operation frame.
2	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`service-discovery operation`	To enable the Service Discovery function and to activate the ITxPT Module Inventory service.
`show service-discovery global`	To display the Service Discovery and the ITxPT Module Inventory settings of the device.

Enabling the Link Status Monitoring per Port

For each required port, activate the ITxPT Module Inventory service to monitor the link status of the port.

Perform the following steps:

Step	Action
1	In the table, in the Link column, select the checkbox for the port.
2	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`service-discovery monitor link`	To activate the ITxPT Module Inventory service to monitor the link status of the port.
`show service-discovery port`	To display the Service Discovery and the ITxPT Module Inventory settings per port.
`exit`	To change to the Configuration mode.

Enabling the PoE Status Monitoring per Port

For each required port, activate the ITxPT Module Inventory service to monitor the PoE status of the port.

Perform the following steps:

Step	Action
1	In the table, in the PoE column, select the checkbox for the port.
2	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface **1/1**.
`service-discovery monitor poe`	To activate the ITxPT Module Inventory service to monitor the PoE status of the port.
`show service-discovery port`	To display the Service Discovery and the ITxPT Module Inventory settings per port.
`exit`	To change to the Configuration mode.

Setting Up the Configuration Environment

Setting Up a DHCP/BOOTP Server

The following example illustrates the configuration of a DHCP server using the haneWIN DHCP Server software as an example. This software is referenced for illustrative purposes only. Equivalent configurations can be implemented using any standard-compliant DHCP server.

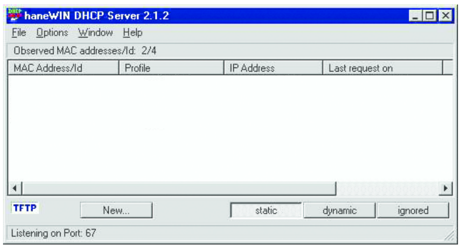
Perform the following steps:

- Install the DHCP server on your PC.

  To carry out the installation, follow the installation assistant.

- Start the haneWIN DHCP Server program.

Start window of the haneWIN DHCP Server program:



Observed MAC addresses/Id: 2/4

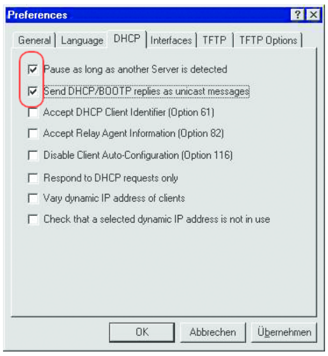
MAC Address/Id	Profile	IP Address	Last request on

Listening on Port: 67

NOTE: When Windows is activated, the installation procedure includes a service that is automatically started in the basic configuration. This service is also active although the program itself has not been started. When started, the service responds to DHCP queries.

- In the menu bar, click **Options > Preferences** to open the program settings window.
- Select the **DHCP** tab.
- Specify the settings displayed in the figure.

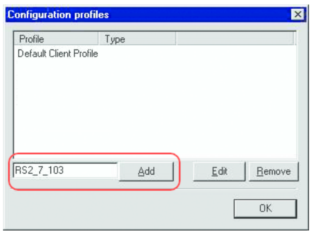
  DHCP setting:



☑ Pause as long as another Server is detected
☑ Send DHCP/BOOTP replies as unicast messages
☐ Accept DHCP Client Identifier (Option 61)
☐ Accept Relay Agent Information (Option 82)
☐ Disable Client Auto-Configuration (Option 116)
☐ Respond to DHCP requests only
☐ Vary dynamic IP address of clients
☐ Check that a selected dynamic IP address is not in use

- Click **OK**.
- To enter the configuration profiles, from the menu bar, click **Options > Configuration Profiles**.
- Specify the name for the new configuration profile.

  Adding configuration profiles:

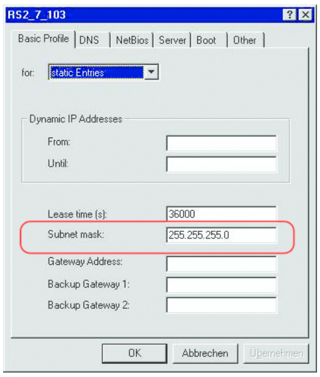


Profile	Type
Default Client Profile	

RS2_7_103

- Click **Add**.
- Specify the netmask.

  Netmask in the configuration profile



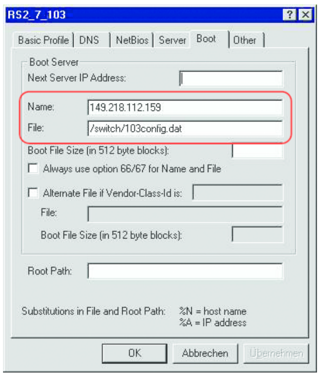
for: static Entries

Lease time (s): 36000

Subnet mask: 255.255.255.0

- Click the Apply button.
- Select the **Boot** tab.
- Enter the IP address of your tftp server.
- Enter the path and the file name for the configuration file.

  Configuration file on the tftp server:


RS2_7_103
Basic Profile
DNS
NetBios
Server
Boot
Other
Boot Server
Next Server IP Address:
Boot File Size (in 512 byte blocks):
☐ Always use option 66/67 for Name and File
☐ Alternate File if Vendor-Class-Id is:
File:
Boot File Size (in 512 byte blocks):
Root Path:
OK
Abbrechen
Übernehmen

Name: 149.218.112.159

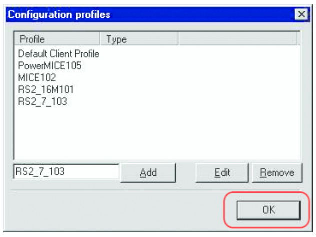
File: /switch/103config.dat

Substitutions in File and Root Path: %N = host name
%A = IP address

- Click **Apply**, then click **OK**.
- Add a profile for each device type.

  When devices of the same type have different configurations, you add a profile for each configuration.

  Managing configuration profiles:

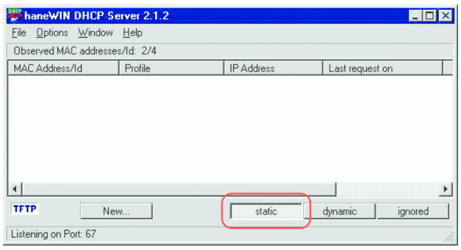


Profile	Type
Default Client Profile	
PowerMICE105	
MICE102	
RS2_16M101	
RS2_7_103	

RS2_7_103

- To complete the addition of the configuration profiles, click **OK**.
- To enter the static addresses, in the main window, click **Static**.

  Static address input:

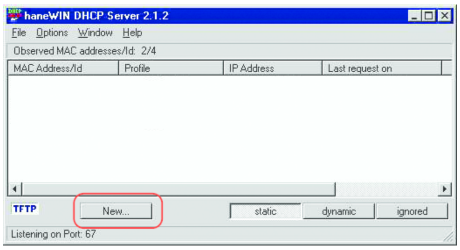


Observed MAC addresses/Id: 2/4

Listening on Port: 67

- Click **Add**.

  Adding static addresses:



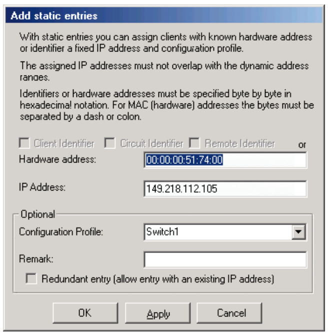
Observed MAC addresses/Id: 2/4

MAC Address/Id	Profile	IP Address	Last request on

Listening on Port: 67

- Enter the MAC address of the device.
- Enter the IP address of the device.

  Entries for static addresses:



With static entries you can assign clients with known hardware address or identifier a fixed IP address and configuration profile.

The assigned IP addresses must not overlap with the dynamic address ranges.

Identifiers or hardware addresses must be specified byte by byte in hexadecimal notation. For MAC (hardware) addresses the bytes must be separated by a dash or colon.

□ Client Identifier □ Circuit Identifier □ Remote Identifier or

Hardware address: 00:00:00:51:74:00

IP Address: 149.218.112.105

Optional

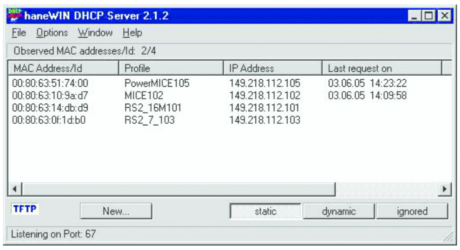
Configuration Profile: Switch1

Remark:

□ Redundant entry (allow entry with an existing IP address)

- Select the configuration profile of the device.
- Click **Apply**, then click **OK**.
- Add an entry for each device that will get its parameters from the DHCP server.

  DHCP server with entries:



Observed MAC addresses/Id: 2/4

MAC Address/Id	Profile	IP Address	Last request on
00:80:63:51:74:00	PowerMICE105	149.218.112.105	03.06.05 14:23:22
00:80:63:10:9a:d7	MICE102	149.218.112.102	03.06.05 14:09:58
00:80:63:14:db:d9	RS2_16M101	149.218.112.101	
00:80:63:0f:1d:b0	RS2_7_103	149.218.112.103	

Listening on Port: 67

Setting Up a DHCP Server With Option 82

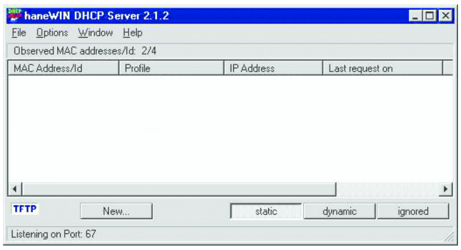
The following example illustrates the configuration of a DHCP server using the haneWIN DHCP Server software as an example. This software is referenced for illustrative purposes only. Equivalent configurations can be implemented using any standard-compliant DHCP server.

Perform the following steps:

- Install the DHCP server on your PC.

  To carry out the installation, follow the installation assistant.
- Start the haneWIN DHCP Server program.

Start window of the haneWIN DHCP Server program:

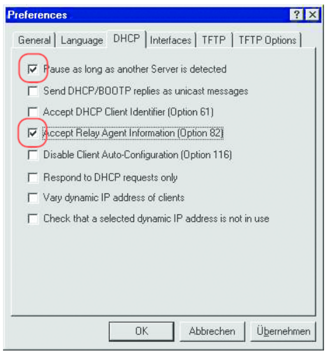


Observed MAC addresses/Id: 2/4

Listening on Port: 67

NOTE: When Windows is activated, the installation procedure includes a service that is automatically started in the basic configuration. This service is also active although the program itself has not been started. When started, the service responds to DHCP queries.

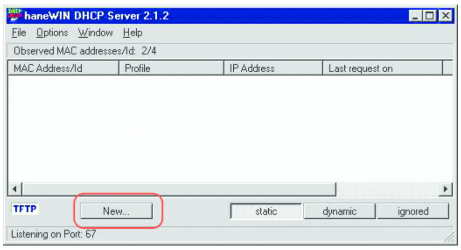
DHCP setting:



☑ Pause as long as another Server is detected
☐ Send DHCP/BOOTP replies as unicast messages
☐ Accept DHCP Client Identifier (Option 61)
☑ Accept Relay Agent Information (Option 82)
☐ Disable Client Auto-Configuration (Option 116)
☐ Respond to DHCP requests only
☐ Vary dynamic IP address of clients
☐ Check that a selected dynamic IP address is not in use

- To enter the static addresses, click **Add**.

Adding static addresses:

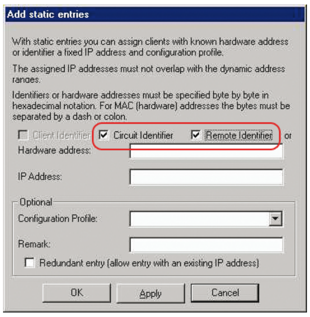


Observed MAC addresses/Id: 2/4

Listening on Port: 67

- Select the Circuit Identifier checkbox.
- Select the Remote Identifier checkbox.

Default setting for the fixed address assignment:



With static entries you can assign clients with known hardware address or identifier a fixed IP address and configuration profile.

The assigned IP addresses must not overlap with the dynamic address ranges.

Identifiers or hardware addresses must be specified byte by byte in hexadecimal notation. For MAC (hardware) addresses the bytes must be separated by a dash or colon.

☐ Client Identifier ☑ Circuit Identifier ☑ Remote Identifier or

Hardware address:

IP Address:

Optional

Configuration Profile:

Remark:

☐ Redundant entry (allow entry with an existing IP address)

- In the **Hardware address** field, specify the value Circuit Identifier and the value Remote Identifier for the switch and port.

  The DHCP server assigns the IP address specified in the **IP address** field to the device that you connect to the port specified in the **Hardware address** field.

  The hardware address is in the following form:

  ciclvvvvssmmpprirlxxxxxxxxxxxx

  - **ci**

    Sub-identifier for the type of the Circuit ID
  - **cl**

    Length of the Circuit ID.
  - Schneider Electric identifier:

    01 when a Schneider Electric device is connected to the port, otherwise **00**.
  - **vvvv**

    VLAN ID of the DHCP request.

    Default setting: **0001** = VLAN 1
  - **ss**

    Socket of device at which the module with that port is located to which the device is connected. Specify the value **00**.
  - **mm**

    Module with the port to which the device is connected.
  - **pp**

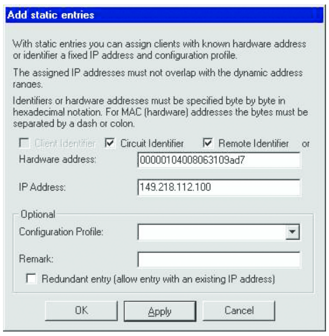
    Port to which the device is connected.
  - **ri**

    Sub-identifier for the type of the Remote ID
  - **rl**

    Length of the Remote ID.
  - **xxxxxxxxxxxx**

    Remote ID of the device (for example MAC address) to which a device is connected.

Specifying the addresses:



Add static entries

With static entries you can assign clients with known hardware address or identifier a fixed IP address and configuration profile.

The assigned IP addresses must not overlap with the dynamic address ranges.

Identifiers or hardware addresses must be specified byte by byte in hexadecimal notation. For MAC (hardware) addresses the bytes must be separated by a dash or colon.

□ Client Identifier ☑ Circuit Identifier ☑ Remote Identifier or

Hardware address: 000001040080631 09ad7

IP Address: 149.218.112.100

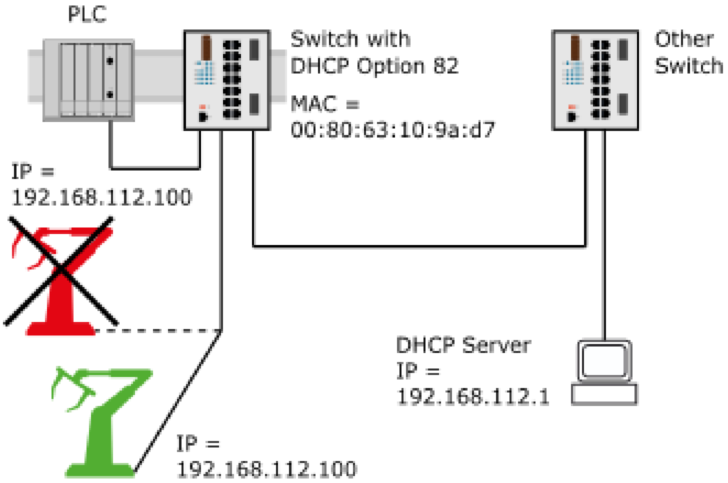
Optional

Configuration Profile:

Remark:

□ Redundant entry (allow entry with an existing IP address)

Application example of using Option 82:



HTTPS Certificate

Your web browser establishes the connection to the device using the Hypertext Transfer Protocol Secure (HTTPS). The prerequisite is that you enable the HTTPS server function in the **Device Security > Management Access > Server**, **HTTPS** tab.

Conflicts in Certificate Validation

Web browsers and other third-party software routinely validate digital certificates.

If your web browser displays a message indicating a conflict in validating the digital certificate of the device, perform the following steps:

- Verify if the digital certificate has expired.
- Verify if your web browser no longer regards the algorithm used for generating the digital certificate as trustworthy.

To solve the conflict in certificate validation, update the digital certificate on the device. For details, refer to HTTPS Certificate Management, page 380.

HTTPS Certificate Management

To establish a secure connection, a digital certificate in X.509 format is required. In the default setting, the device uses a self-signed digital certificate.

You can regenerate the self-signed digital certificate using the latest device software.

Perform the following steps:

Step	Action
1	Navigate to the **Device Security > Management Access > Server**, **HTTPS** tab.
2	To generate a self-signed digital certificate, in the Certificate frame, click **Create**.
3	To apply the settings, click the ✓ button.
4	For the changes to take effect after transferring a digital certificate onto the device, disable and re-enable the HTTPS server. Restart the HTTPS server using the Command Line Interface.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`https certificate generate`	To generate a digital certificate for the HTTPS server.
`no https server`	To disable the HTTPS function.
`https server`	To enable the HTTPS function.

As an alternative, generate a digital certificate externally, using up-to-date signature algorithms. Transfer the new digital certificate onto the device. To do this, perform the following steps:

Step	Action
1	Navigate to the **Device Security > Management Access > Server**, **HTTPS** tab.
2	When the file is located on your PC or on a network drive, drag and drop it onto the ⤒ area. As an alternative, click in the area to select the file.
3	To transfer the file to the device, click **Start**.
4	To apply the settings, click the ✓ button.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`copy httpscert envm <file name>`	To transfer the digital certificate for the HTTPS server from the external memory (**ENVM**) onto the device.
`configure`	To change to the Configuration mode.
`no https server`	To disable the HTTPS function.
`https server`	To enable the HTTPS function.

NOTE: To activate the digital certificate after the device generated or you transferred it, reboot the device or restart the HTTPS server. Restart the HTTPS server using the Command Line Interface.

Access Through HTTPS

The default setting for HTTPS data connection is TCP port **443**. If you change the number of the HTTPS port, reboot the device or the HTTPS server. Thus the change becomes effective.

Perform the following steps:

Step	Action
1	Navigate to the **Device Security > Management Access > Server**, **HTTPS** tab.
2	Enable the HTTPS function. Select the **On** radio button in the Operation frame.
3	To access the device by HTTPS, enter HTTPS instead of HTTP in your web browser, followed by the IP address of the device.

Execute the following commands:

Command	Description
`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`https port 443`	To specify the number of the TCP port on which the web server receives HTTPS requests from clients.
`https server`	To enable the HTTPS function.
`show https`	To display the status of the HTTPS server and the port number.

When you make changes to the HTTPS port number, disable the HTTPS server and enable it again to make the changes effective.

The device uses Hypertext Transfer Protocol Secure (HTTPS) and establishes a new data connection. When you log out at the end of the session, the device terminates the data connection.

Appendix

Management Information Base (MIB)

The Management Information Base (MIB) is designed in the form of an abstract tree structure.

The branching points are the object classes. The "leaves" of the MIB are called generic object classes.

When this is required for unique identification, the generic object classes are instantiated, that means the abstract structure is mapped onto reality, by specifying the port or the source address.

Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The object description or object ID (OID) identifies the object class. The subidentifier (SID) is used to instantiate them.

Example:

The generic object class **sa2PSState** (**OID** = **1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1**) is the description of the abstract information **power supply status**. However, it is not possible to read any value from this, as the system does not know which power supply is meant.

Specifying the subidentifier **2** maps this abstract information onto reality (instantiates it), thus identifying it as the operating status of power supply **2**. A value is assigned to this instance and can be read. The instance **get 1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1** returns the response **1**, which means that the power supply is ready for operation.

The following table gives the definition of the syntax terms used

Syntax term	Definition
Integer	An integer in the range **$-2^{31}..2^{31}-1$**
IP address	**xxx.xxx.xxx.xxx** (**xxx** = integer in the range **0..255**)
MAC address	12-digit hexadecimal number in accordance with ISO/IEC 8802-3
Object Identifier	x.x.x.x… (for example 1.3.6.1.1.4.1.3833...)
Octet String	ASCII character string
PSID	Power supply identifier (number of the power supply unit)
TimeTicks	Stopwatch, Elapsed time = numerical value / 100 (in seconds) Numerical value = integer in the range **$0..2^{32}-1$**
Timeout	Time value in hundredths of a second Time value = integer in the range **$0..2^{32}-1$**
Type field	4-digit hexadecimal number in accordance with ISO/IEC 8802-3
Counter	Integer (**$0..2^{32}-1$**), when certain events occur, the value increases by **1**.

List of RFCs

The following table describes the list of RFCs:

RFC	Description
RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2613	SMON
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2863	The Interfaces Group MIB

RFC	Description
RFC 2865	RADIUS Client
RFC 2866	RADIUS Accounting
RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 2869bis	RADIUS support for EAP
RFC 2933	IGMP MIB
RFC 3164	The BSD syslog protocol
RFC 3376	IGMPv3
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3580	802.1X RADIUS Usage Guidelines
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 3621	Power Ethernet MIB
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4188	Definitions of Managed Objects for Bridges
RFC 4251	SSH protocol architecture
RFC 4291	IPv6 Addressing Architecture
RFC 4252	SSH authentication protocol
RFC 4253	SSH transport layer protocol
RFC 4254	SSH connection protocol
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4318	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 4861	Neighbor Discovery for IPv6
RFC 5321	Simple Mail Transfer Protocol
RFC 6221	Leightweight DHCPv6 Relay Agent
RFC 8200	IPv6 Specification
RFC 8415	DHCPv6

Underlying IEEE Standards

The following table describes the underlying IEEE standards:

Standard	Description
IEEE 802.1AB	Station and Media Access Control Connectivity Discovery
IEEE 802.1D	MAC Bridges (switching function)
IEEE 802.1Q	Virtual LANs (VLANs, MRP, Spanning Tree)
IEEE 802.1X	Port Authentication
IEEE 802.3	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet

Underlying IEC Norms

The following table describes the underlying IEC norm:

Norm	Description
IEC 62439	High availability automation networks MRP – Media Redundancy Protocol based on a ring topology

Underlying ANSI Norms

The following table describes the underlying ANSI norm:

Norm	Description
ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

Technical Data

Switching

The following table described the switching parameters:

Parameter	Value
Size of the MAC address table (forwarding database) (incl. static filters)	16384
Max. number of statically set-up MAC address filters	100
Max. number of MAC address filters learnable through IGMP Snooping	1024
Max. number of MAC address entries (MMRP)	64
Number of priority queues	8 Queues
Port priorities that can be set	0..7
MTU (Max. allowed length of packets a port can receive or transmit)	9720 Bytes

VLAN

The following table describes the VLAN parameters:

Parameter	Value
VLAN ID range	1..4042
Number of VLANs	max. 128 simultaneously per device max. 128 simultaneously per port

Access Control Lists (ACL)

The following table describes the Access Control Lists:

Description	Value
Max. number of ACLs	50
Max. number of rules per ACL	512
Max. number of rules per port	512
Number of total configurable rules	4096 (8 × 512)
Max. number of VLAN assignments	24
Max. number of rules which log an event	128
Max. number of Ingress rules	514

Copyright of Integrated Software

The product contains, among other things, Open Source Software files developed by third parties and licensed under an Open Source Software license.

You can find the license terms in the Graphical User Interface in the **Help > Licenses** dialog.

Abbreviations used

ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DUID	DHCP Unique Identifier
EUI	Extended Unique Identifier
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv6	Internet Protocol version 6
LDRA	Lightweight DHCPv6 Relay Agent
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol
NDP	Neighbor Discovery Protocol
NMS	Network Management System
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted-pair

UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

Index

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

QGH59056.03